Omni-Series

User's Manual

Copyright © 1991-2011 XLink Technology, Inc.

XLink Technology, Inc.
www.xlink.com

Phone: (408) 263-8201
Fax: (408) 263-8203
Sales e-mail: sales@xlink.com
Support e-mail: support@xlink.com

Copyright Notice

All rights reserved. Reproduction or use of editorial or pictorial content in any manner without expressed permission is prohibited. Use, copy, and disclosure are restricted by license agreement.

Trademarks

Omni-NFS, Omni-NFS/X, Omni-NFS Enterprise, Omni-NFS/X Enterprise, Omni-VT420, Omni-Tar, Omni-NFS Gateway, Omni-NFS Dual Gateway, Omni-Print, Omni-Lite ,and Omni-Series related products are registered trademarks of XLink Technology, Inc..
Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other trademarks or registered trademarks of respective holders are acknowledged.

Table of Contents

CHAPTER 1 ..... *1*

HOW TO USE THIS MANUAL *1*

INTRODUCING OMNI-SERIES SOFTWARE *1*
ABOUT OMNI-SERIES *1*
OMNI-SERIES PACKAGES *2*
ADDITIONAL INFORMATION *2*
CONVENTIONS USED IN THIS USER'S GUIDE *3*

CHAPTER 2 ..... *5*

NFS GATEWAY *5*

INTRODUCTION *5*
DEFINE THE NFS SERVER SYSTEMS *6*
OPTIONS OF NFS GATEWAY *10*
MAPPING FOR GATEWAY NETWORK USERS *11*
HOW NFS GATEWAY LICENSE WORKS *13*

CHAPTER 3 ..... *15*

NFS DUAL GATEWAY *15*

INTRODUCTION *15*
STARTING NFS DUAL GATEWAY *16*

CHAPTER 4 ..... *17*

NFS CLIENT *17*

INTRODUCTION *17*
SETUP NFS CLIENT CONNECTION *17*
Using NFS client tool: *18*
Set up "auto mount" *22*
Access NFS server system from Network Neighborhood: *23*
Command line of "net use" *23*
SYMBOLIC LINKS *23*

CHAPTER 5 ..... *25*

NFS SERVER *25*

INTRODUCTION *25*
USING NFS SERVER SOFTWARE FOR WINDOWS 2008/7/2003/2000/XP/NT *26*
Export drives or a folders for NFS sharing *26*
Exporting Network Drives *28*
Understand Concept Of Mapping *29*
Setup Mapping *30*
Options for NFS server *36*
Share NFS printers *39*
USING NFS SERVER SOFTWARE FOR WINDOWS 98/95/ME *39*
SETUP MAPPING *41*
Working with Security *42*
Options for NFS Server *43*
Setup NFS Printer *44*
Utility for NFS Server *44*
Auto Start NFS Server Service *47*

CHAPTER 6 ..... *49*

HOST EDITOR *49*

INTRODUCTION *49*
SETUP HOST EDITOR *49*
NIS SETUP *52*

CHAPTER 7 ..... *53*

LPD SERVER *53*

INTRODUCTION *53*
CONFIGURE XLPD SERVER *53*
Setup *54*
Viewing the queue *56*
Change printer port *57*
Edit a printer setting *57*
Print to a file *58*
General Trouble Shooting *58*

CHAPTER 8 ..... *61*

LPR HOSTS *61*

INTRODUCTION *61*
STARTING LPR HOSTS *61*

CHAPTER 9 ..... *63*

ADDING NETWORK PRINTERS *63*

INTRODUCTION *63*
SETTING UP AND USING NFS PRINTER *63*
Remote Printer Name *63*
Adding NFS Printer To a Windows system *64*
SETTING UP AND USING LPR PRINTER *65*
TROUBLESHOOTING *66*

CHAPTER 10 ..... *67*

FTP SERVER *67*

INTRODUCTION *67*
CONFIGURE FTP SERVER *68*

CHAPTER 11 ..... *71*

FTP CLIENT *71*

INTRODUCTION *71*
USING FTP CLIENT *71*
TROUBLESHOOTING *76*

CHAPTER 12 ..... *77*

VT420 (TELNET) *77*

INTRODUCTION *77*
USING VT420 TERMINAL EMULATION *77*
MULTIPLE SESSION CAPABILITY *78*
STARTING AND TERMINATING VT420 ..... *78*
GENERAL SETUP *79*
DISPLAY SETUP *82*
KEYBOARD SETUP *84*
AUTO LOGIN *85*
PRINTER SETUP *86*
KEYMAP *86*
COLOR MAPPING SETUP *88*
Assigning colors to individual text attributes *88*
TROUBLESHOOTING *89*

CHAPTER 13 ..... *91*

RSH (REMOTE SHELL) *91*

INTRODUCTION *91*
USING RSH *91*

APPENDIX A ……..93

NETWORK LOCK MANAGER (NLM FILE LOCKING) 93

FILE LOCKING..... 93
NO LOCKING 94
READ ONLY..... 94

APPENDIX B..... 95

PCNFSD..... 95

PCNFSD PROTOCOL DEFINITION..... 95
AUTHENTICATION 95
PRINT SPOOLING..... 96

APPENDIX C..... 97

HOW TO SETUP LPR ON REMOTE UNIX SYSTEMS... 97

APPENDIX D..... 99

EXAMPLES ON HOW TO START NFS SERVER ON A UNIX SYSTEM..... 99

APPENDIX E..... 101

THE SYSTEM SETTINGS FOR CROSS DOMAIN FILE ACCESS WITH NFS SERVER PRODUCT 101

For Windows NT server 101
For Windows 2000 server 102

APPENDIX F..... 103

FIREWALL SETUP ON WINDOWS XP AND VISTA SYSTEMS..... 103

GLOSSARY *107*

INDEX *109*

CHAPTER 1

How to Use this Manual

Introducing Omni-Series Software

Omni-series software is a set of computer software products that utilize NFS protocol for Windows ⇔ Unix systems connectivity. Following topics are illustrated in this chapter:

- **About Omni-Series Software –** describes the Omni-Series software and lists some of the features.
- **Omni-Series Packages –** lists all the packages available in the Omni-Series software family.
- **Additional Information** – describes where additional information can be found.
- **Conventions used in this User's Guide** – describes the conventions used throughout this Guide along with any other assumptions that should be noted by the Omni-Series software users.

About Omni-Series

The Omni-Series software provides you with easy and efficient tools to operate and manage your network environment. A wide variety of applications are designed to make better use of existing resources by implementing file and print sharing within your network.

Omni-Series software works in conjunction with Microsoft's TCP/IP. It is a combination of comprehensive NFS and network related applications, which transform your PC into a fully functional NFS client/server.

Omni-Series Packages

For Windows 2000/NT

Package Name	*Related Application Reference*
Omni-NFS Gateway	Chapter 2, 6 -13
Omni-NFS Dual Gateway	Chapter 2, 3, 5 -13

For Windows 2003/2000/NT/98/95/XP/ME

Package Name	*Related Application Reference*
Omni-NFS Enterprise	Chapter 4 -13
Omni-NFS/X Enterprise	Chapter 4 -13
Omni-NFS Server	Chapter 5, 6, 7, 10
Omni-Print	Chapter 6, 7, 8, 9
Omni-VT420	Chapter 6, 11, 12
Omni-X	Refer to Omni-X User Manual
Omni-Lite	Chapter 4, 6, 7, 8, 9

For Windows 98/95/ME

Package Name	*Related Application Reference*
Omni-NFS	Chapter 4 -13

Additional Information

The Omni-Series software comes with comprehensive and easy to use online help. Changes and additions to any of the applications will be announced on XLink's web site and are downloadable. Some examples are also provided and accessible from our web FAQ page.

If you have any technical question or problem that needs to be resolved immediately, our support staff can be reached via e-mail or by phone for one-on-one troubleshooting.

Note: The content information in this User Guide may be updated without notice. Addendum may be requested.

You can contact XLink's Technical Support Department, Monday to Friday between 9:00a.m. and 6:00p.m. Pacific standard time (with the exception of holidays) at:

XLink Technology, Inc.
1677 South Main Street
Milpitas, CA 95035
U.S.A.

Phone: 408-263-8201
Fax: 408-263-8203
E-mail: support@xlink.com
WEB: http://www.xlink.com

Conventions Used In This User's Guide

This guide provides instructional-based information. The following table provides some conventions used throughout this Guide.

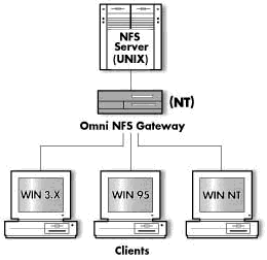
If you see…	*It means….*
<ret>	Press "Enter" key on your keyboard.
<tp> xxxx	Type the subsequent character with your keyboard.
<pc>	Indicates commands on your PC
<ux>	Indicates commands on your UNIX hosts
C:>	DOS command prompt
#	UNIX command prompt
Bold	Any word in bold type indicates important or specific terminology used in Windows or Omni-NFS Series software, or dialog button names.
eg.	Indicates example.
Note:	Side notes or tips.
<Data>	< > indicated information needs to be entered.

CHAPTER 2

NFS Gateway

Introduction

Omni NFS Gateway is a NFS client product with gateway functionalities. Installed on a Windows 2000/NT server system, it allows NFS connections being re-shared to all Windows workstations in the LAN as local drives.



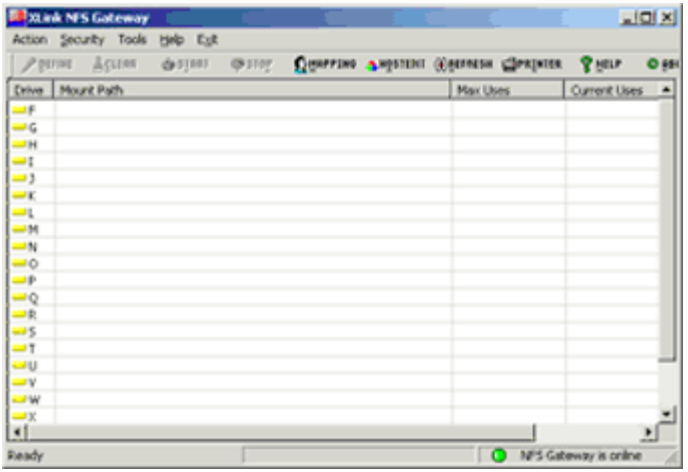
Administrators can now gain centralized network control. It provides **Transparent**, **Secure**, and **User-friendly** access for users to NFS resources. Files remain on the NFS host system, so Windows and UNIX users gain access to files without duplicating data. Individual Windows user identities are mapped to NFS accounts as they are passed through the Gateway, ensuring security and restricting file access privileges.

In this chapter, following subjects will be explained in details:

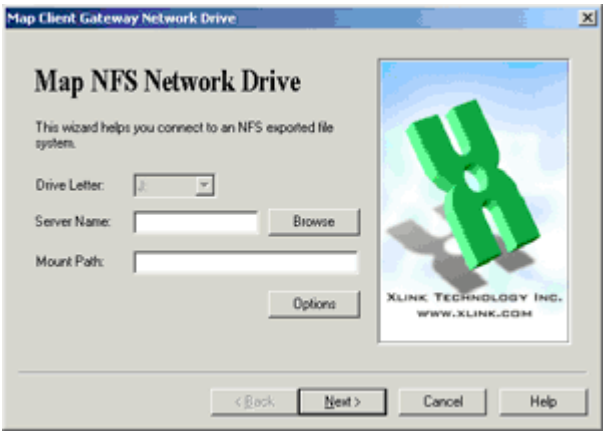
- Define the NFS Server systems
- Options
- Mapping
- Licensing

Define the NFS server systems

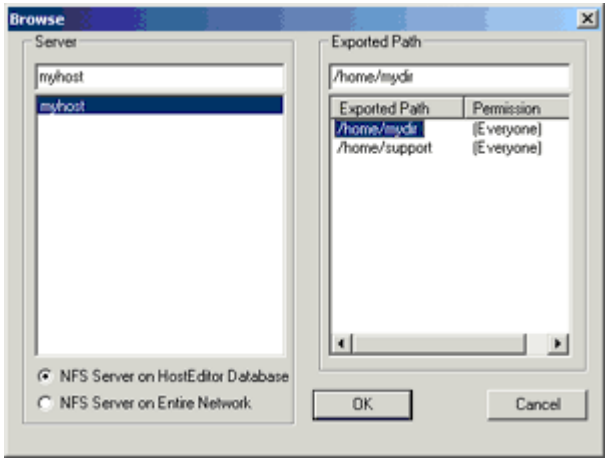
NFS Gateway, functioning as a NFS client, needs to define NFS server systems before connections can be established.



From NFS Gateway's user interface window shown above, (assume you have setup Host Editor) select a "drive", then click on the 'define' button to bring up next dialog box.

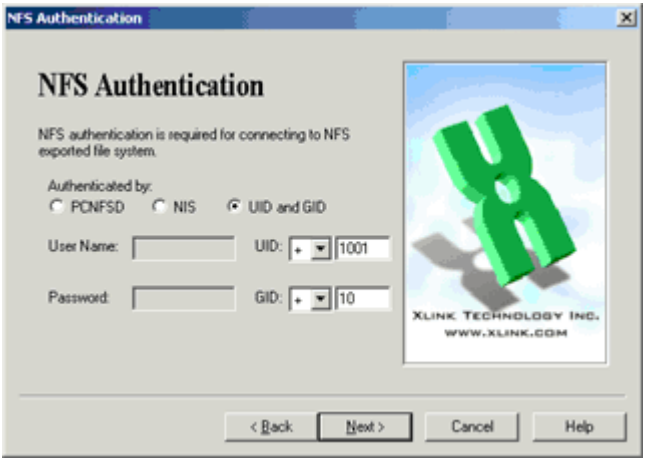


Click on 'Browse' to open up next dialog box which lists all NFS server systems defined in Host Editor.



Select the one you want to connect to. By clicking on the system name, you will bring out the exported directory of the system. Select the exported path and click 'OK' to close the box and 'Authentication' dialog box should appear.

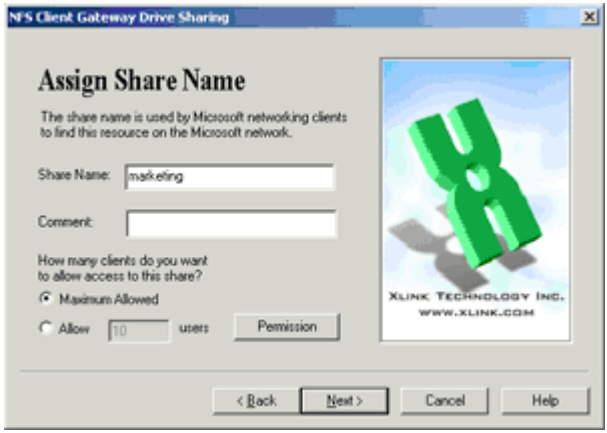
There are three ways to setup the authentication for access permission to the NFS connection. The first two choices require you to enter a NFS server's user account and its password. To use PCNFSD method, you need to have the 'pcnfs' daemon running on the NFS server system. To use NIS method, you need to have the NFS server (in Host Editor) setup first.



The last authentication method is 'UID and GID'. They are the user id and group id numbers of an account on the NFS server system.

The user account used to mount the NFS drive on the NFS Gateway will be referred to as the default user account. Any user accessing NFS based files or data through Gateway 2000/NT Server without proper user identification mapping will have the default user access right. This is an advantage for administrators to better manage unknown or unauthorized user access to the NFS resources. It is advisable to use a low privilege default user account.

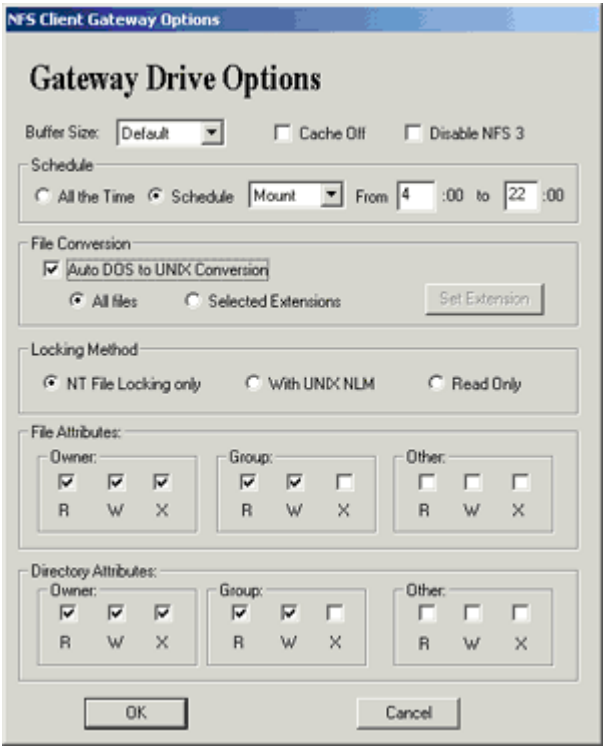
Click 'Next' to bring up next dialog box. Here you can change the mounted drive letter to a name that is easy for you to remember. And you can specify the number of users to be allowed to share the mounted drive on the Gateway.



By click on button ‘Permission’, administrator can configure user access permissions to the re-shared NFS drives in addition to the standard NFS permission. Administrator can add, remove, or set specific restrictions and access permissions to the selected drives using standard Microsoft security feature.

Close this dialog box and click 'Next' to finish up setting 'define'.

Options of NFS Gateway



The features of NFS Gateway options are:

- **Buffer size:** Adjust the buffer size can help to improve file transfer rate and sometimes improve data quality.
- **Cache Off:** With the box unchecked, data can be stored in local cache memory. When it is checked, the data from NFS drive will be retrieved directly form NFS server.
- **Disable NFS 3:** By default NFS 3 is on. This means NFS 3 on the NFS server system is required. If you are sure that NFS 2 is running on the NFS server system, check the box.

- **Schedule:** This feature allows user to specify mount/umount time for better service control, the 'military time' (0-23 hours) is used here.

- **File Conversion:** File conversion is bi-directional. It replaces the LF of a DOS file with a 'space' for UNIX viewing; and replace the EOL character of a UNIX file with a CR character for Windows viewing. The replacements is done to keep the file size unchanged.

  It is not recommanded to turn on this option which might cause corruption with none ASSCII files. If not all files with different files extensions are wanted for file conversion, the "Set Extension" button will allow you to select desired files by their extensions.

- **Locking Method:** With the selection, NFS client place the request for the type of service.

- **File attributes:** All files created in the mounted drive will match the settings here.

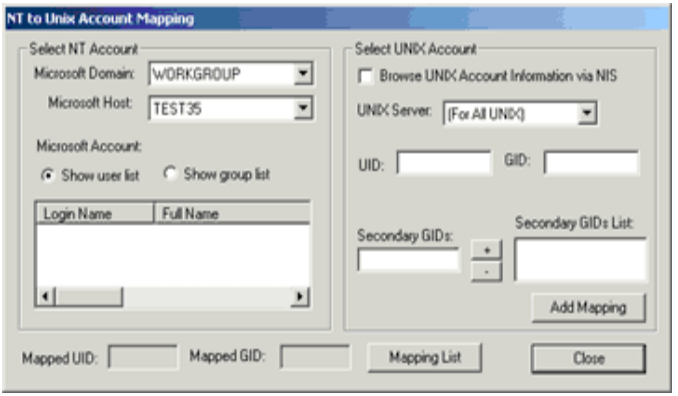
- **Directory Attributes:** All directions created in the mounted drive will match the settings here.

Mapping for Gateway network users

While the 'Authentication' set in both 'HostEditor' and 'Define' are for Gateway connecting to the NFS server, you need to setup 'Mapping' to give access permission to the Windows network users who want to access files on the NFS server system through the Gateway.

To setup 'Mapping', you need to first create user accounts on the Gateway system for each Windows user in the subnet, and also create user accounts for them on the NFS server system. Then map them up.

For example, the five Windows systems in the subnet having the login accounts: John, Jay, Jessica, Janet and Joan. You will create five user accounts on the Gateway system: J1, J2, J3, J4 and J5, and five user accounts on the NFS server system j1, j2, j3, j4 and j5.



Then, from this dialog box, the default should show correct domain and host name (the Gateway system) in Microsoft Domain and Microsoft Host. From Microsoft Accounts list, you select J1 and enter j1's user id and group id numbers in 'UID' and 'GID' screens. You can specify the NFS server system or leave it default as 'For All Unix'. Click on 'Add Mapping' to complete setting.

If J1 on the Gateway system and j1 on the NFS server system are the accounts assigned to John, then with the setting, John will be able to access the mounted drive on the Gateway system by login as J1, and work with files on the NFS server system created by j1. The rest of the 'mapping' for all other accounts will follow suit.

NFS Gateway also allows Group Account Mapping. To map a group of users in selected Microsoft Host, you will need to bring up the Mapping Dialog. You can view the group lists on a selected host by clicking on the **Show group list** radio button (to map the entire group with a unique UID & GID, you need to highlight a group from the list then assign UID & GID by manually type in or from NIS list).

Accounts mapped for all users can be viewed by clicking on the **View Mapped Log** button.

How NFS Gateway license works

NFS Gateway provides service of NFS connections to other Windows systems in the subnet. With this design, a 5-user license of Omni NFS Gateway means one installation on a Windows NT or 2000 server system, and five connections from other Windows systems in the subnet. The user connection is concurrent.

CHAPTER 3

NFS Dual Gateway

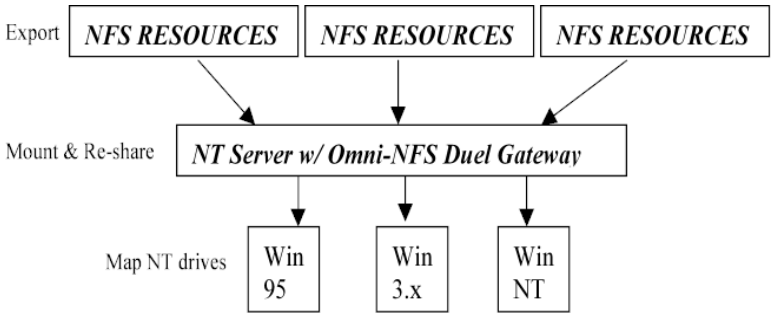
Introduction

Omni NFS Dual Gateway is an extended package from Omni NFS Gateway. By including a NFS server in the product, Omni NFS Dual Gateway allows file sharing for both directions.

It provides **Transparent, Secure**, and **User-friendly** access for users to NFS resources. Files remain on the NFS host system, so Windows and UNIX users gain access to files without duplicating data. Individual Windows user identities are mapped to NFS accounts as they are passed through the Gateway, ensuring security and restricting file access privileges.

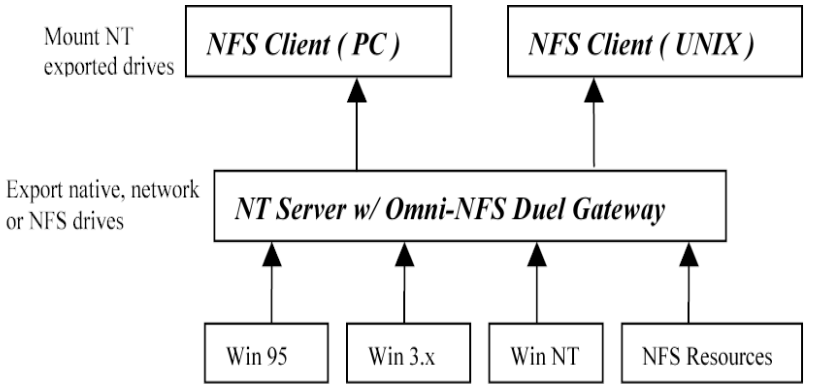
Client Gateway Service

Provides re-sharing services for Windows Clients to access NFS resources from 2000/NT Gateway Server.



Server Gateway Service

Administrators can also export any 2000/NT drives to the authorized UNIX or PC Clients through NFS using Server Gateway.



Starting NFS Dual Gateway

Please refer to Chapter 2 (NFS Gateway) for the Client Gateway configuration and Chapter 5 (NFS Server) for the Server Gateway configuration.

CHAPTER 4

NFS Client

Introduction

NFS Client enables users of Microsoft Windows systems to gain access to the NFS file systems on UNIX networks.

This chapter explains how to access those remote files.
NFS Client provides you with the following advantages:

- You can now use all Microsoft Windows operating systems to access data/files located on the UNIX platforms. Windows applications now can directly work with the file while it is still on the UNIX machines. No need to FTP files back and forth.
- You can save hard drive space by keeping the file on the UNIX server.
- Seamless integration with the Windows platform enables users to access UNIX files easily via Windows Explorer, Network Neighborhood, and My Computer.

Setup NFS Client Connection

NFS Client enables Windows users to gain access to UNIX drives as any typical Windows network drive. This means that there's no need to transfer files residing on the UNIX machines (NFS Server) to the local computer in order to work with them.

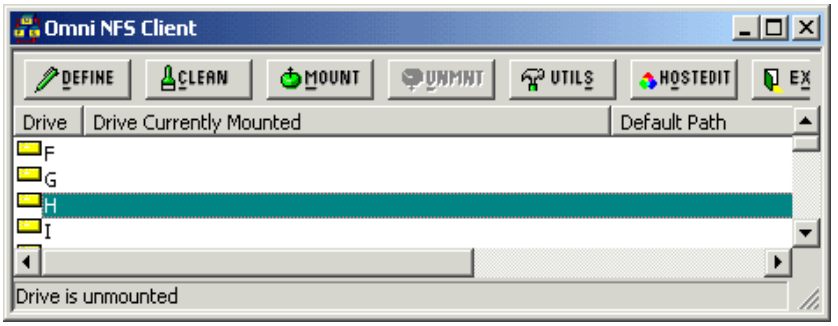
With Xlink NFS client application installed and Host Editor properly configured, a user can access the NFS server system in three ways:

1. Run NFS Client's user interface tools for NFS connection
2. Utilize Windows Network Neighborhood
3. Run the 'net use" command line in Windows Command Prompt

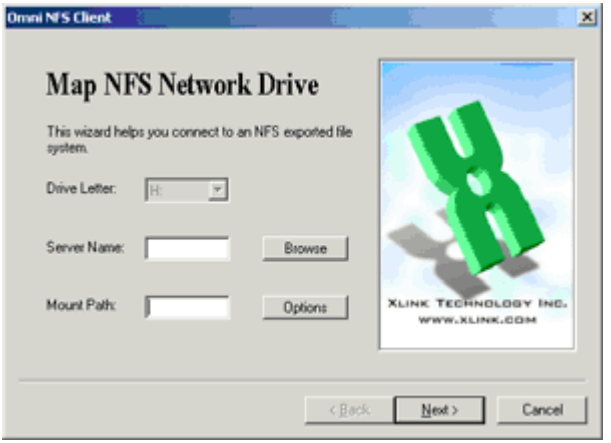
You can set auto mount when mounted with NFS client's tools. With this setting, the mounted drives will be listed under 'my computer' of windows explorer every time when the system is turned on.

Using NFS client tool:

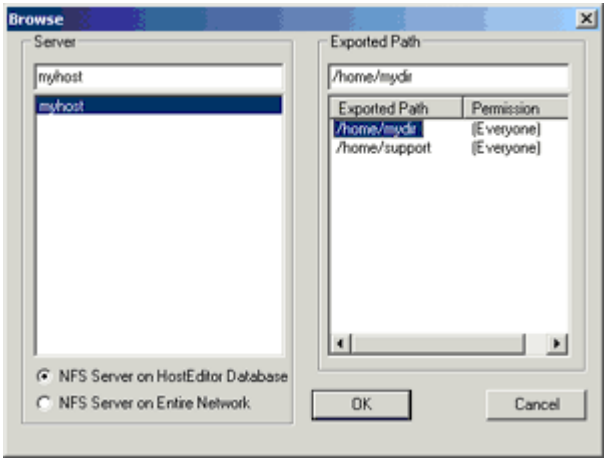
From windows 'Start' menu select 'Programs/Omni Lite/NFS Client'. Following user interface window will come up.



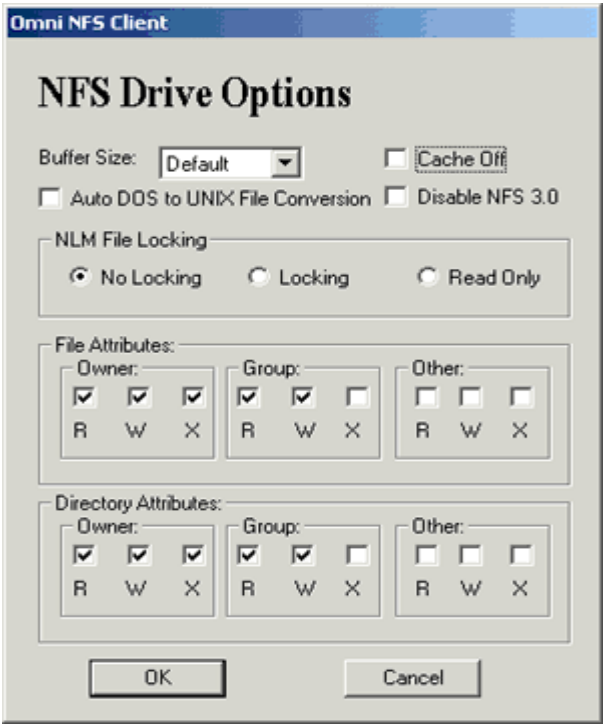
(Assume you have setup Host Editor) Select a "drive" from the user interface window then click on the 'define' button to bring up next dialog box.



Click on 'Browse' to open up next dialog box with all remote system defined in Host Editor listed. Select the one you want to connect to. By clicking on the system name, you bring out the exported directory of the system. Select the directory and click 'OK' to close the dialog box.



Now you are back to the first dialog box, click on 'options' to bring up next dialog box.



The option selections:

Buffer size: adjust buffer size can help to improve file transfer rate and sometimes improve data quality.

Cache Off: turn off cache to enable real time data updates but might decrease performance

Disable NFS 3: by default NFS 3 is on

File Conversion: File conversion is bi-directional. It replaces the LF of a DOS file with a 'space' for UNIX viewing; and replace the EOL character of a UNIX file with a CR character for Windows viewing. The replacements is done to keep the file size unchanged.

It is not recommanded to turn on this option which might cause corruption with none ASCII files. If not all files with different files extensions are wanted for file conversion, the "Set Extension" button will allow you to select desired files by their extensions.

Locking Method: record locking to be supported only when application used supports the function

File attributes: all files created in the mounted drive will match the settings here

Directory Attributes: all directions created in the mounted drive will match the settings here

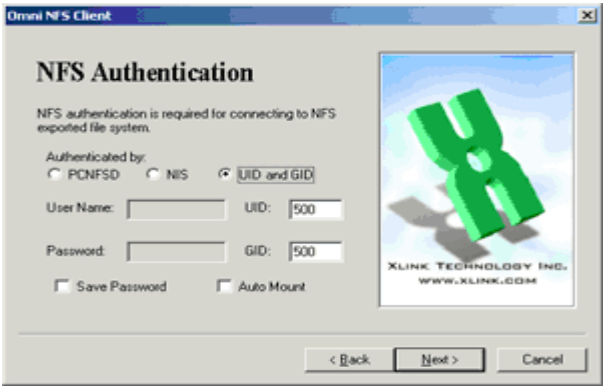
Click 'OK' to close the dialog box. From the first box again, click 'next' to setup the authentication.

There are three ways to setup the authentication for access permission to the NFS connection. The first two choices require you to enter a user account and its password. To use PCNFSD method, you need to have the 'pcnfs' daemon running on the NFS server system. To use NIS method, you need to have the NFS server (in Host Editor) setup first.

The last authentication method is 'UID and GID'. UID and GID are the user id and group id numbers of a UNIX account.

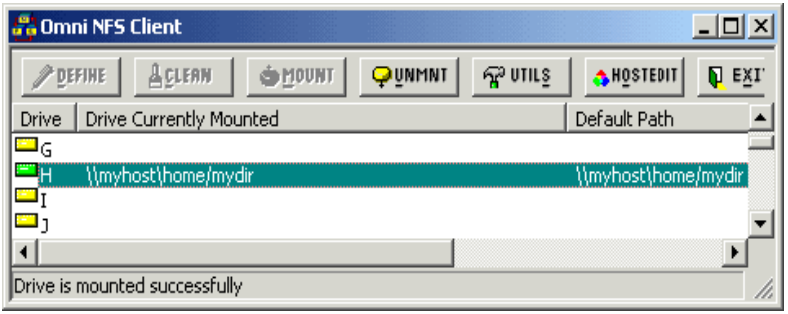
The AutoMount here, when checked, will do the mounting action for you every time when the NFS client user interface is opened with the NFS server and exported directory path defined.

Note: AutoMount is active only when Save password box is also checked.



Click 'Next' and 'Finish' to complete the 'define' configuration.

When you are back to the NFS client user interface window, click on 'mount' to make the connection. If all settings are correct, you should see the drive and path listed as in the following picture. Now from windows explorer, you will see drive "H" listed under My Computer.



Set up "auto mount"

Host Editor must be correctly set and its interface window closed.

In window explorer, select 'Tools/Map Network Drive'. In the dialog box, select a drive, select from dropdown menu or type in the exported path in unicode (ie. \\host\exported directory).

Check the box 'reconnect at logon' and click 'OK'.

when the dialog box closed up, in windows explorer you will see the mounted drive under My Computer.

Access NFS server system from Network Neighborhood:

Double Click the "My Network Neighborhood" icon on the desktop.

Double click "Entire Network and then "Xlink_NFS". This window should list all of the NFS Servers you have setup in "Host Editor".

Select the NFS server you wish to mount and double click to bring up the exported directories.

You can then access the files created by the authenticated user. The authenticated user is the user account you used for authentication when setup Host Editor.

Command line of "net use"

Assume there is an exported directory "myexport" in the /export directory of the NFS server system named "mynfs.

To establish NFS server connection, type: net use \\mynfs\myexport

Once the connection is established, you can use Command Prompt's commands to access files in the NFS server system.

Symbolic Links

NFS Client will automatically get the final target file for a symbolic link if the paths for the symbolic link and those target files are both exported.

Example:
File /usr1/test is pointed to /usr2/test.
Linked /usr2/test will only be seen on mounted drive only if both /usr1 and /usr2 directories are exported on the remote system.

CHAPTER 5

NFS Server

Introduction

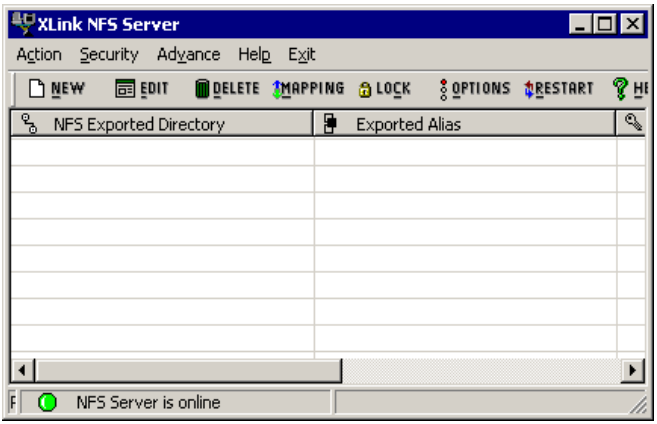
Omni NFS Server software turns your Microsoft Windows system into a NFS server system so that remote UNIX and other NFS client systems can share files and printers on your system. On Windows 2008/7/2003/XP /2000/NT/9x systems, NFS server service is started automatically with the system. Except in one occasion when server option "Enable Xlink Portmapper" is changed, changes made in server configuration require no restart of NFS server service.

With the same basic functionalities, NFS server for Windows 2008/7/2003/ 2000/XP/NT has a different user interface tool than that for Windows 98/95 and ME systems. The first part of this chapter will be focusing on NFS server for 2008/7/2003/2000/XP/NT systems. If you need help for NFS server for 98/95 and ME systems, please turn to page 35.

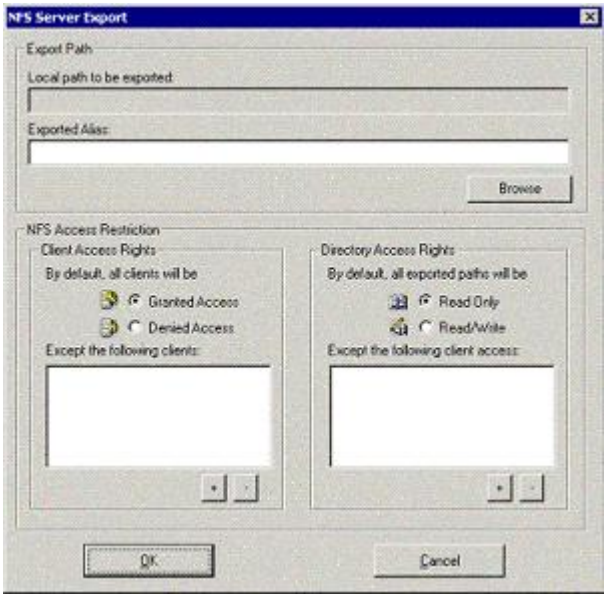
Using NFS Server software for Windows 2008/7/2003/2000/XP/NT

Export drives or a folders for NFS sharing

Following is the user interface window for Omni NFS server for Windows 2008/7/2003/2000/XP/NT systems.


XLink NFS Server
Action Security Advance Help Exit
NEW EDIT DELETE MAPPING LOCK OPTIONS RESTART
NFS Exported Directory
Exported Alias
NFS Server is online

From this user interface window, click on 'New' to export local or network drive/folders for NFS connection.



Click on 'Browse' to select drive or folders to be exported. You can assign alias name for the exported path by changing the exported path in 'exported alias' window to the name desired. This name can then be used in the 'mount' command line for NFS connection. (Alias can also be used to avoid the drive letter (required by windows) in 'mount' command line)

For example: the exported path is c:\myfolder\mytest, and alias 'mypath' is assigned. The mount command line can then be:

mount myserver:/mypath /mountpoint

In 'NFS Access Restriction' area, select the radio buttons for desired settings on both 'client Access rights' and 'Directory Access Rights'. With no specific client systems listed, all clients have the same permission as set. Click on "+" button to add client systems.

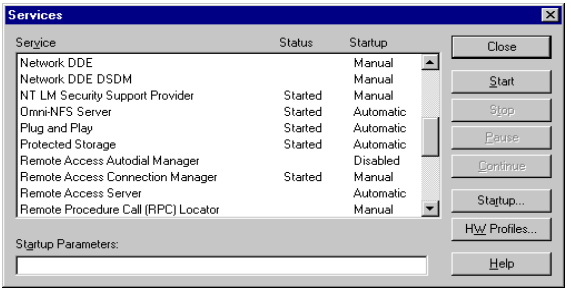
Please note: the settings are in "exception" formatting.

For example, if 'myclient' is added to the client list with radio button 'Granted Access' selected, the server is set **not** to allow connection request from 'myclient'.

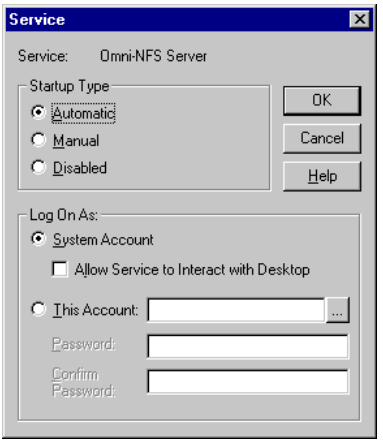
Exporting Network Drives

Special setting is needed if Windows network drives are to be exported through NFS Server Service. Before exporting a network drive, please perform the following steps:

1. Go to **Control Panel/ Services** and select **Omni-NFS Server**.



2. Click on the **Startup** to modify the settings.



3. In the **Log On As** group box, select **This Account**.

4. If the account name is not set to **Administrator**, you will need to click on the list button to get a list of accounts.

5. Select **Administrators** followed by the **Add** button to set the account name and click **OK** to validate your changes.

6. Once all the setting is set, restart the **Omni-NFS Server** service.

Note: *The passwords of the administrator accounts for both local system and the peer workstation from which the network drive is mapped have to be the same.*

Understand Concept Of Mapping

Why mapping:

With more network security concerns, better protections are implemented on computer systems. While Windows NTFS file system has tighter security checkups than the original FAT file system, Omni NFS server, the windows application, needs to follow suit. Mapping is the Omni NFS server's approach in complementing windows NTFS security system.

Two ways to map:

There are two ways to set 'mapping' in NFS server: universal mapping and one-to-one mapping. The universal mapping is a way to "disable" NFS server user checkup. The user's group, however, still needs to be defined. With this setting, all users belong to the group can access the mounted directory.

The one-to-one mapping creates a tighter check on access right for NFS client users. With this setting, each user on the NFS client system must be mapped to one account on the NFS server system. Once connected, the user on the NFS client system will be able to access files created by the mapped account on the NFS server system.

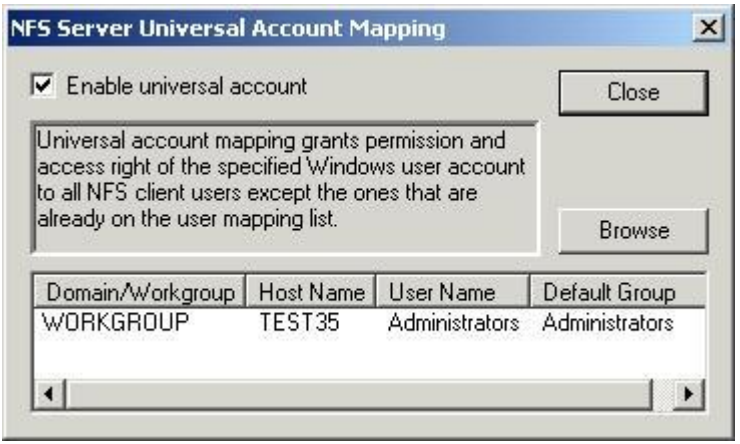
Setup Mapping

The Universal Account

The universal mapping is a way to "disable" NFS server user checkup. The user's group, however, still needs to be defined. With this setting, all users belong to the group can access the mounted directory.

1. Click button from the “mapping” box to open his dialog box, check the box “Enable universal account” and then “browse” for local account
2. Do the “group name to GID mapping” like you did above

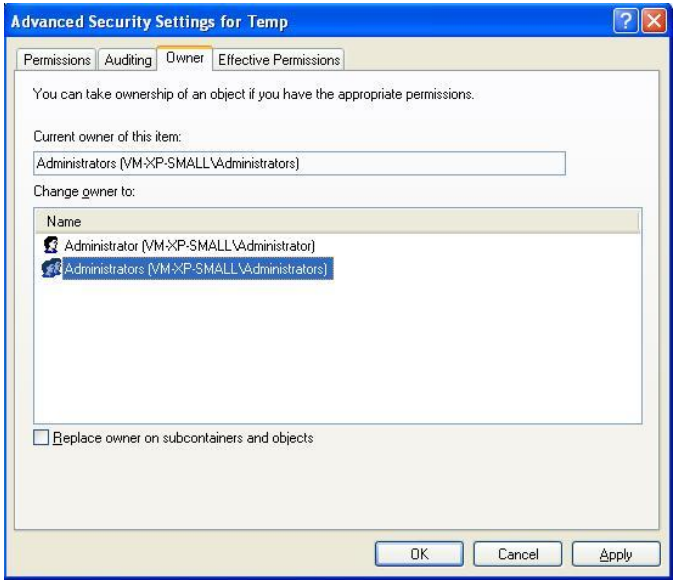
3. The 'Universal mapping' will not show up in the 'mapping' dialog box. It is in effect when you click on the 'Close' button. Universal mapping will override on-to-one mapping if both are set.



The one-to-one mapping

1. Find out the owner account of the exported path

You need to use the owner account to set up either UID/GID mapping or universal mapping latter on. For example , if the owner of the exported path is “local machine\administrators”, you will provide “local machine\administrators” for user mapping. If you provide domain administrator in mapping setup, the mapping may fail to work.



How to find out the owner of a folder

- On Windows 2008/7/2003 -

  1. Highlight the exported folder
  2. Right mouse
  click **property** => **security** => **Advanced** => **Owner**

- On XP -

  Step 1: goto **Control Panel** => **Folder Options** => uncheck **clear Use simple file sharing [Recommended]**
  Step 2: Following instructions On Windows 2003 above

2. Decide to use either UID/GID mapping or universal mapping

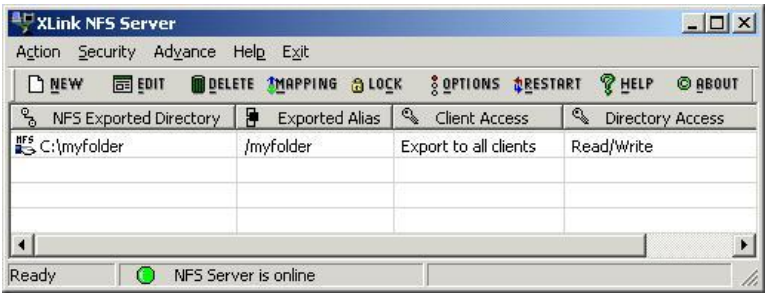
Each UNIX account has a GID number and UID number. You may login a UNIX account and type `id` to see the UID and GID of the current login UNIX account. The `User Mapping` is for you to map a windows account to a UNIX account. It is used to solve the security issue between windows and UNIX systems.

The individual UID/GID mapping is one to one. If you want all UNIX accounts to have the windows "administrator" permission to access the exported path, you can turn on "universal mapping" instead of using individual UID/GID mapping.

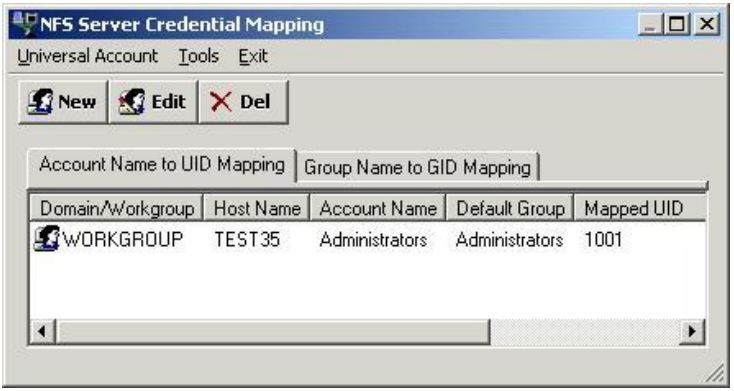
3. The user mapping procedures

You need to know the owner account of the exported path before starting to set up the user mapping.
With following user mapping, it allows a mapped UNIX account to access all files created by the owner in the exported path.

The following are instructions:

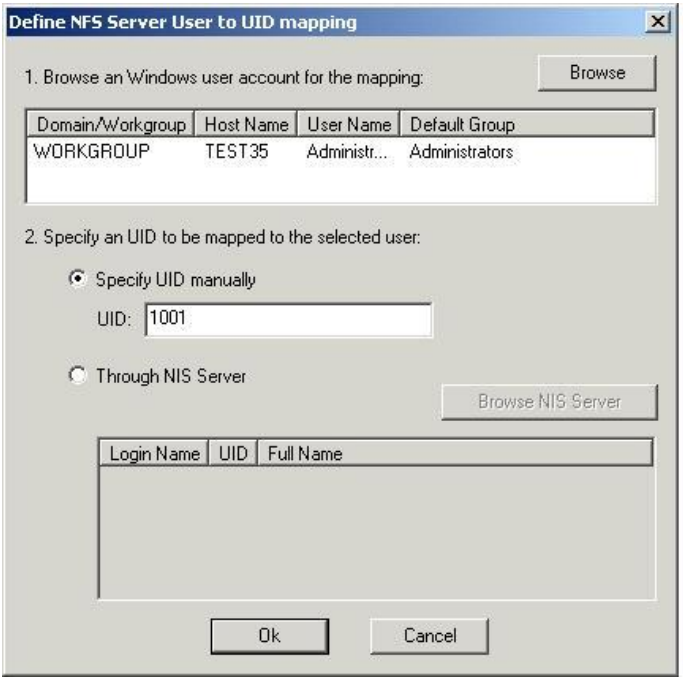


Open up NFS server GUI, and click the button “mapping” to open next dialog box You have the choice of mapping a specific **UID/GID client account** OR the **universal account.**

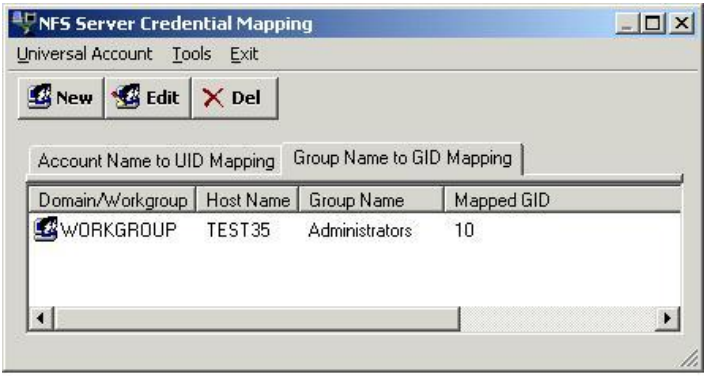


- **UID/GID mapping**

  To map a specific client account to NFS server,
  1• click button “New” for next dialog box
  2• click “Browse” to select local account (this is the account that creates the exported drive/folder)
  3• enter the client account’s user id number (the account that is going to access the mounted directory on the UNIX system), click “OK”



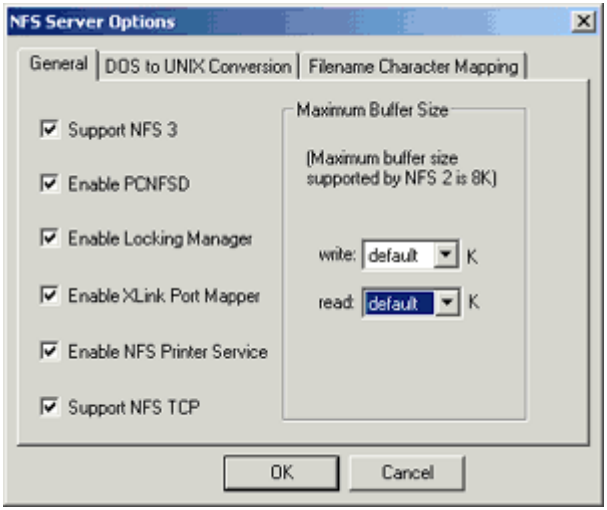
Select “Group Name to GID Mapping”,
1• Click button “New” and “browse” to find local account’s group
2• Enter the UNIX account’s group id number
3• Click “OK”



Options for NFS server

Click on 'Options' from the NFS server interface window to setup server options. Three dialog boxes are provided for easy setup.

In the 'General' dialog box:



In details:

Support NFS 3: With this box checked, NFS server service is up to NFS 3. When it is unchecked, NFS server service is up to NFS 2 only.

Enable PCNFSD: This box is checked to allow NFS client using PCNFS authentication method for security checking.

Enable Locking Manager: When this box is check, the NFS client's request of file locking can be serviced.

Enable Xlink Port Mapper: Have this box checked to use NFS server's own portmapper. Turn it off when there is already a portmapper running on the system. NFS server can utilize third party portmapper.

NFS server service must be restarted every time when there is a changed made on this check box.

Enable NFS Printer Service: With this box checked, NFS server will automatically export NFS printer to all clients in the subnet. If this is not desired, uncheck the box.

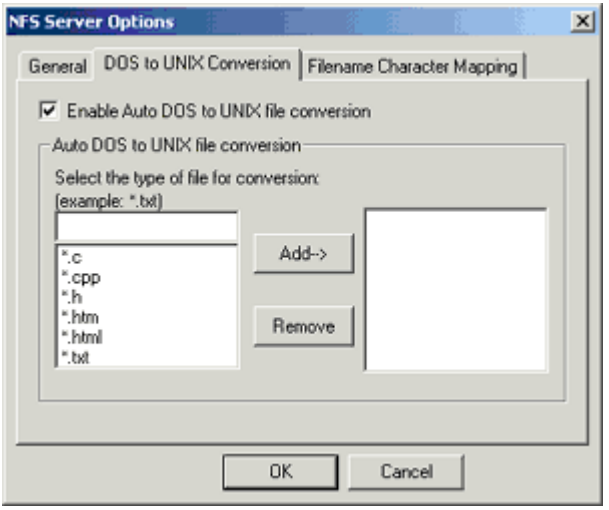
Support NFS TCP: With this box checked, NFS server can take both TCP and UDP service request. Uncheck the box if only UDP connection is needed.

The default buffer size is automatically set to the maximum available buffer according to your system configuration. However, default buffer size might not be the best option for all system environments. Modifying the buffer size can sometimes increase file transfer rate, and even improve data quality.

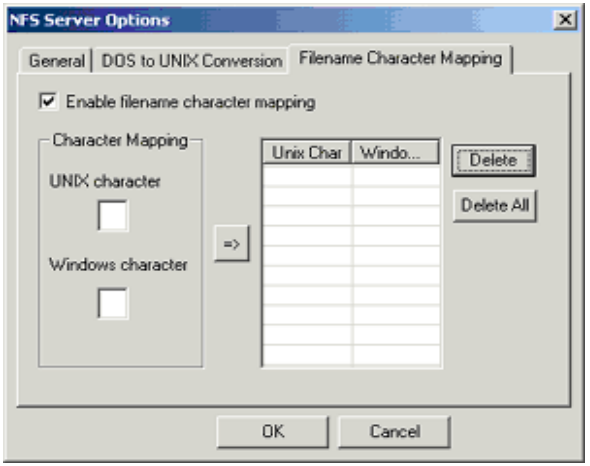
Please note: the maximum buffer size for NFS2 is 8kb. The maximum buffer size for NFS3 is 64kb. To adjust buffer size, the recommended size is 4kb.

In 'DOS to UNIX Conversion' dialog box.

Check the ‘Enable Auto DOS to UNIX file conversion’ box to enable this feature. File extensions need to be added for the file conversion to be effective. It is recommended to set this option on text files only because non-text file might be corrupted by the conversion.



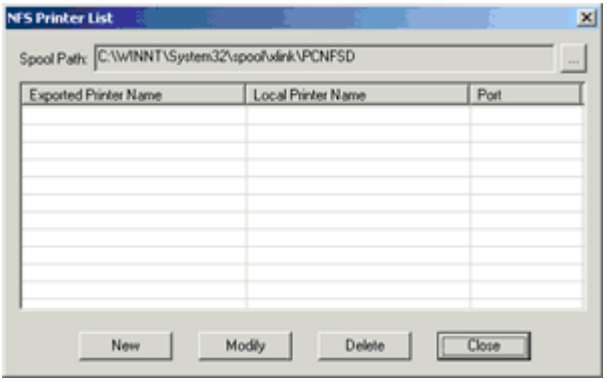
In 'Filename Character Mapping' dialog box:



Check the box to enable the 'character mapping' feature. Enter UNIX and Windows characters you want to map, and click on the '=>' button to complete the setting.

Share NFS printers

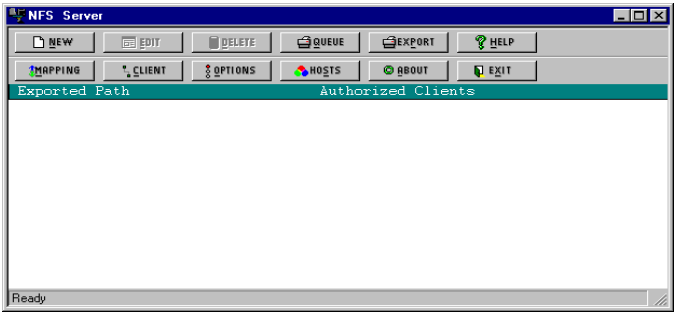
From NFS server user interface windows, click on 'Advance' button in tool bar, then select 'NFS Printer/Printer config' to bring up next dialog box.



Click 'New' to add NFS printers. The spool path can be changed by click on the button next to it.

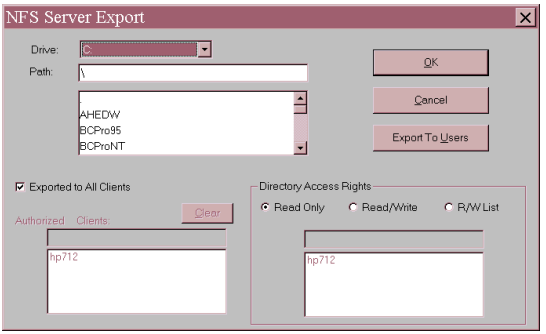
Using NFS Server software for Windows 98/95/ME

The **NFS Server** application is used to view the status of exported paths, define exported paths and exported printer and show printer queue status. Once you have defined or modified a resource within the **NFS Server** application, you need to restart the **NFS server** to activate them.



Please perform the following steps in order to export Windows resources to remote NFS clients:

1. Click on the **New** button to start defining a new exported path. **NFS Server** then uses this information to export the resource you have defined when you restart the **NFS Server**.
2. In the **NFS Server Export** dialog box, select the path to be exported, including drive and directory.



By default, the **Export to All Clients** box is checked. If this path is restricted to certain remote hosts for access, uncheck the **Export to All Clients** and enter the host names (or IP) which you have previously defined in the **Host Editor** to be **Authorized Clients.**

If you want to export your file system to specific users use **Export to Users** (this option is only available for Win95/98/ME version of NFS Server). Please refer to the **Security Mapping** section.

3. The **Directory Access Rights** privilege setting defaults to **Read Only** for all authorized clients. You can grant read/write privilege to all authorized clients by selecting **Read/Write** radio button. In case you would like to grant read/write privilege to any of the authorized clients, simply check the **R/W List** radio button, and double click on the client in the list below. Any authorized client not selected in the **R/W List** setting will have Read Only privilege. Notice that each authorized client granted the Read and Write privilege is separated by a comma (,).

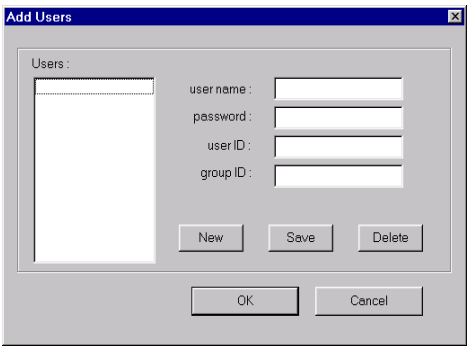
4. When all the parameters are correctly entered, press **OK** to save all definitions. The NFS Server window will then show the parameters that you have defined.

5. The changes to the export function will not be operational until NFS Server restarts.

6. You can repeat the procedure to define as many export paths as you require. You may modify existing resource definitions that you need to change by clicking on the **Edit** button.

Setup Mapping

You may specify each user's read and write permission to your exported path. To add users with specific read/write permission, click on the **Mapping** button from the main NFS Server interface or click on **Export to Users** button on the **NFS Server Export** dialog. A user's authorization always takes precedence over a host's authorization. For example, if a user can read and write to a directory, then both read and write permission are authorized to this user, regardless of the permission authorized to the host from which the user is connected.



Working with Security

In order to keep the security structure of both the NFS Server and UNIX based system on the same ground, the security mapping structure is designed as UNIX file and security permission.

eg. Assuming c:/temp has been mounted to /mnt on UNIX machine with Read/Write permission.

UNIX Information Table

User / UID	**Groups / (GID)**
Root / 0	Sys / 2, root / 0, bin / 3, user / 20, staff /50
John / 100	user / 20
Mary / 103	user / 20, staff /50

NT Information Table

User	**Groups**
Administrator	Administrators, Power User, User, Operator, Engineer
John	User
Amy	User, Engineer

UID Mapping

UNIX UID	**NT User**	**Default Group**
0	Administrator	Administrators
100	John	User
103	Amy	Engineer

GID Mapping

UNIX GID	**NT Group**
0	Administrators
20	User
50	Engineer

NT File Permission

C:\temp (owner = Administrators)	Everyone full control

Once the drive is mounted, anyone who is on the mapping list will have Read/Write permission. Others will only have read permission since NFS Server cannot determine file permission setting with incomplete user information.

If **root** on UNIX machine creates a file, then the file security structure will be:

On UNIX	**On NT**
Owner = root, group = root	Owner = Administrators, group = Administrators
(permission depends on UNIX file mask)	

If you would like to have a group of users to access a specific directory, you can either assigned one user account for all the members of the group, perform mapping for each member and set the group permission accessible, or setup universal account for any file transaction.

*eg. John creates a **Staff** directory on the mounted volume and set the group permission to read/write/execute. Since John's default group is set to **User**, the directory will be accessible to members in **user** group; therefore, any user with **User** default group is included.*

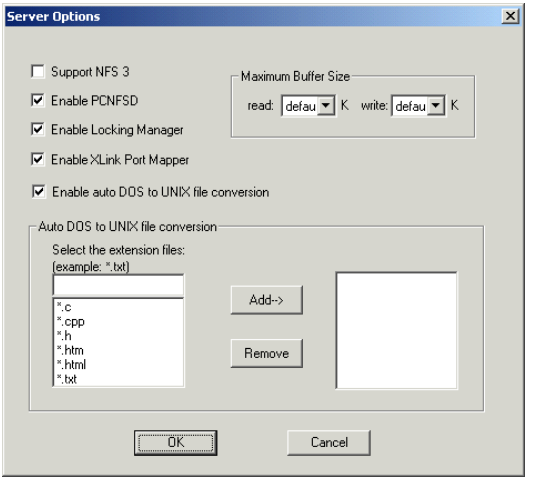
If the owner or the group is viewed as **Nobody** or numbers on the UNIX client, then the mapping is either incomplete or failed. Please check the correct ownership of the file or directory for proper access permission.

Even if you are a super user account on the UNIX machine, you have to perform the security mapping to gain the proper permission.

Note: If you want to connect to the NFS server using PCNFSD from the remote NFS Client, you must know both the user name and password of your NT account to do a successful mount. Since UNIX operating systems use UID and GID as user identity, and UID/GID are not supported by Windows 2000/NT/XP, you must map UID and GID into NT user accounts. By doing so, NFS server can determine the access permissions for each request from the NFS client. Mapping for users who are members of Administrators group will fail except Administrator account.

Options for NFS Server

By pressing the **Option** button, the following dialog box appears:



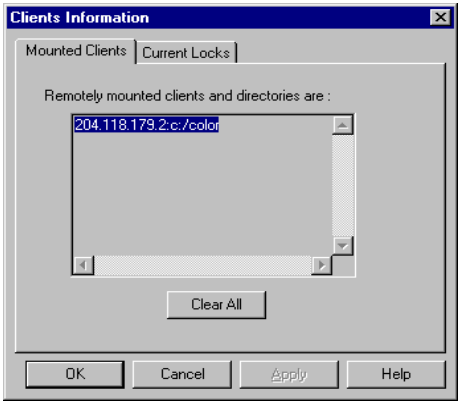
This dialog allows you to enable or disable NFS version 3.0, PCNFSD, Network Locking Manager, Xlink Port Mapper or Auto DOS to UNIX file conversion. You can specify the buffer size as well. After you have changed these options, you must restart the NFS Server service to have the changes take effect. The default setting is everything enabled.
You can also modify the buffer size at run time from **Performance Tips** program (please refer to **Appendix C** for more detail information).

Setup NFS Printer

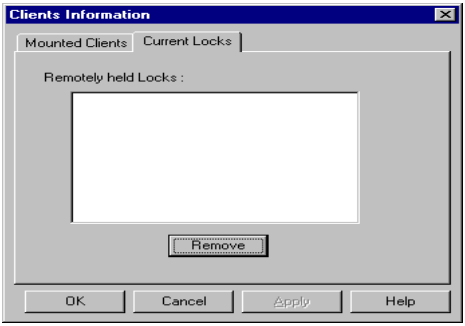
You may setup NFS printer server on your system by clicking on the **Export** button from the NFS Server main interface. On the Exported Printer dialog, click on **New** button to add an NFS printer server entry. You may modify or remove any existing entry with the corresponding buttons. To view the print job queue for any defined NFS printer server, click on the **Queue** button from the NFS Server main interface. You may pause, remove, resume or modify printer setting on **NFS Printer Queue** dialog.

Utility for NFS Server

Clicking the **Client** button will allow you to browse and modify two things: current mounts and current locks.



Current mounts will show you who is currently connected to the NFS Server.



Current locks will show you the file locks currently held by remote clients.

The mounts are saved in the file **mountd.list**. Sometimes if a client does not mount or unmount when it cannot access the NFS server across the network, or an unmount request is not sent correctly, a stale entry can be left in the mountd.list file. When you are sure there are no clients connecting to your NFS server, you can click "Clear All" to remove all the stale entries. Clear mount entries will cause the NFS Server to rebuild its internal file caching structure. Make sure to disconnect any NFS links prior to clearing mount entries.

The current locks show all the locks currently held by remote clients. These locks will recover themselves after a server crash or restart. If the clients crash or restart, they can still hold some locks and in this case, you must remove the locks manually from this dialog page.
The removed locks will be removed from the system the next time you start the NFS server service.

Auto Start NFS Server Service

NFS Server on Windows 98/95/ME can be set to start at boot time by checking the "**Restart at Boot Time**" option with the NFS Server service icon in the system tray.

CHAPTER 6

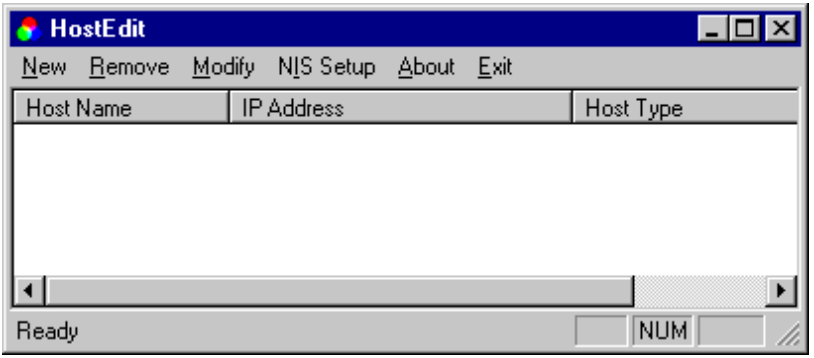
Host Editor

Introduction

The **Host Editor** utility is used to create a host table on your local system, which is used by many Omni-NFS components such as NFS client, NFS Server, VT420, FTP client, etc.

Setup Host Editor

To add a new host to the host table, click on the **Host Editor** icon. The Host Editor dialog box will pop up.



Please perform the following steps to add a new host entry:

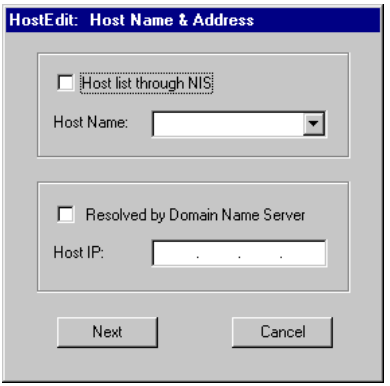
1. Click on the **New** menu to define a new host or double click on any of the existing listing (if previously added) to **Modify** settings for any selected host.

At the **Host Name & Address** dialog box (see picture in next page), enter a name (anything you want to call it) for the Unix system in Host Name. (***Note****: The same host IP can be listed multiple times with different Host*

Names.) This name will be displayed in the Host Editor host list. Then you enter the IP address of the remote host to which you are trying to connect.

If you are authenticating through the NIS Server, and have set up the NIS Server settings in the **NIS Setup** menu (please see next session for details), check the **Host List Through NIS** box, and select the host from the drop down list.

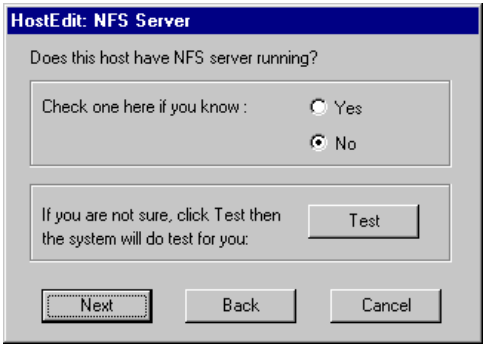
For Host IP, if you do not know the IP address of the remote host but know the real host name, enter the exact real host name in the **Host Name** field, and check the **Resolved by Domain Name Server** box to get the Host IP.



If you are running NFS client product, you will need to do following steps by click on the "Next" button. For all other products, Host Editor definition ends here. The "Next" button is now showing "Close", and by click on it, you indicate the finish of Host Editor definition job.

2. In next dialog box, click on the **Test** button to check if NFS server function is running on the NFS server system. If the NFS server function is active, the *Yes* radio button will be selected for you, and you may proceed by clicking the **Next** button. Otherwise the radio button will stay at "No". You will then need to manually start the NFS server function to run NFS client program.

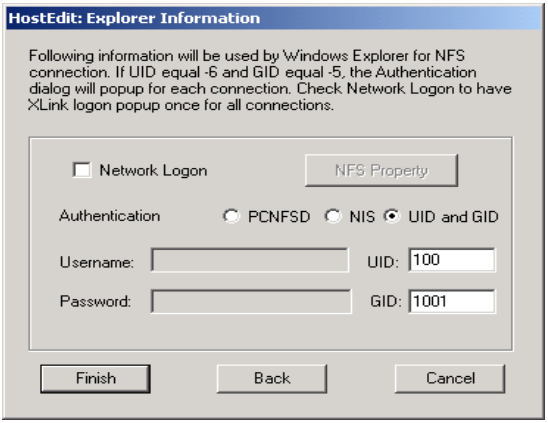
Examples on how to start NFS server on some Unix systems are listed in **Appendix D**.



3. In the **Explorer Information** dialog box, the file access authentication is assigned. The default authentication method is PCNFSD. With this radio button checked, enter the *User Name* and *Password* of your account on the NFS server system.

   If your NFS server system doesn't have PCNFSD installed, you will get an error message later. One way to get around it is to use UID/GID method. Select this radio button, and enter the UID and GID numbers of your account on the NFS server system will get you though this part of the setting.

   Note: To get UID/GID numbers, you login the NFS server system with your account, then type "id" at the prompt.

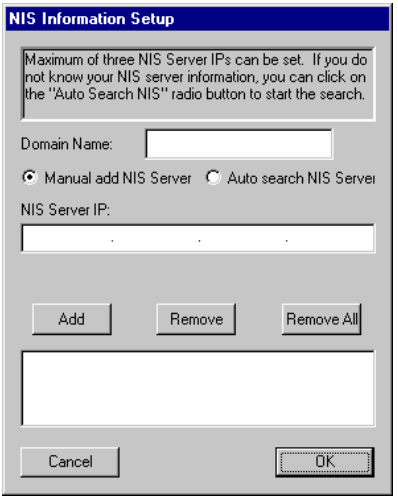

HostEdit: Explorer Information
Following information will be used by Windows Explorer for NFS connection. If UID equal -6 and GID equal -5, the Authentication dialog will popup for each connection. Check Network Logon to have XLink logon popup once for all connections.
Network Logon
NFS Property
Authentication
PCNFSD
NIS
UID and GID
Username:
UID: 100
Password:
GID: 1001
Finish
Back
Cancel

See next session (in next page) for details on NIS setup.

If **Network Logon** is checked, **XLink Logon Window** will popup once to prompt for Username and Password when making all NFS connections. The **NFS Property** button allows you to set properties such as file name creation case for drives mounted through Windows Explorer or Network Neighborhood.

NIS Setup

Click **NIS Setup** button to setup your NIS domain and NIS server address. Host Editor allows user to get specific host information from the NIS host list.


NIS Information Setup
Maximum of three NIS Server IPs can be set. If you do not know your NIS server information, you can click on the "Auto Search NIS" radio button to start the search.
Domain Name:
Manual add NIS Server
Auto search NIS Server
NIS Server IP:
Add
Remove
Remove All
Cancel
OK

CHAPTER 7

LPD Server

Introduction

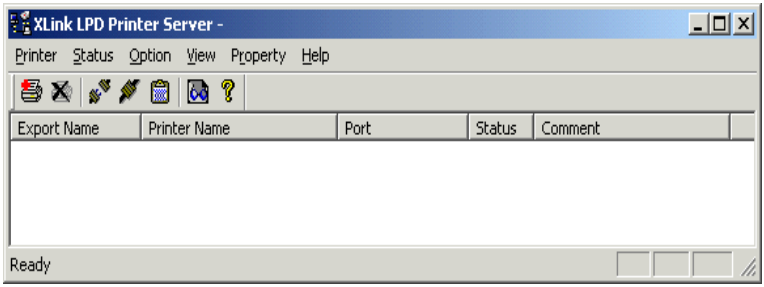
LPD server application provides UNIX print spooling services on your Windows operating systems. LPD accepts print jobs from many hosts or users on the network, queues the jobs and then sends them to any printer attached to the host running LPD.

To send a printing job from a Unix system to a remote printer attached to a Windows system with Xlink LPD installed, a standard Unix print command will do the job.

An added feature of "virtual printer" makes Xlink LPD more versatile. A file on the remote LPR client system can be sent to a specified folder on the LPD server system for later printing.

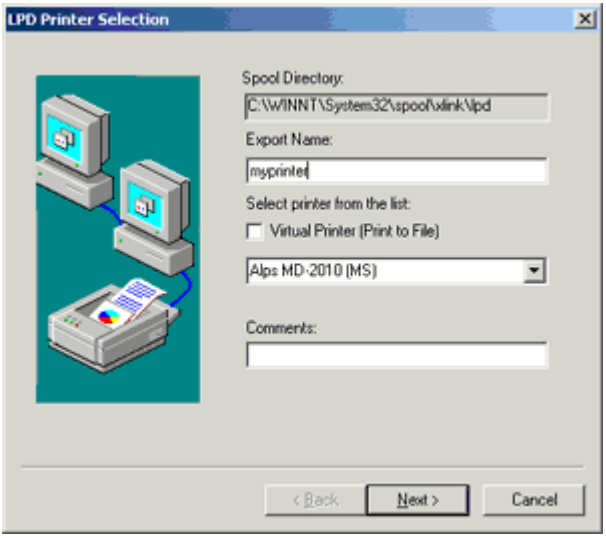
Configure XLPD server

XLink LPD will automatically configure your system after installation. It generates a **spool** directory to store print jobs under your install directory. Make sure that there is an adequate amount of free disk space available in the installation drive. Printer queue names defined in the LPD are the remote queue names defined in the remote LPR clients.

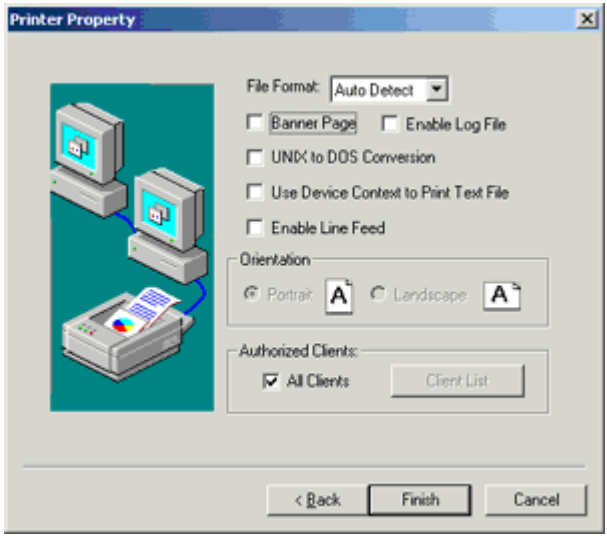


Setup

Click on 'Printer/New' to define a printer. In next dialog box, enter a name in 'Export Name' for the printer you want to share out. Click on the drop-down menu to select the printer.



Click on 'Next' to set the printer options.



File Format

Auto Detect: This is the default setting and in general will detect the format of a printing job.

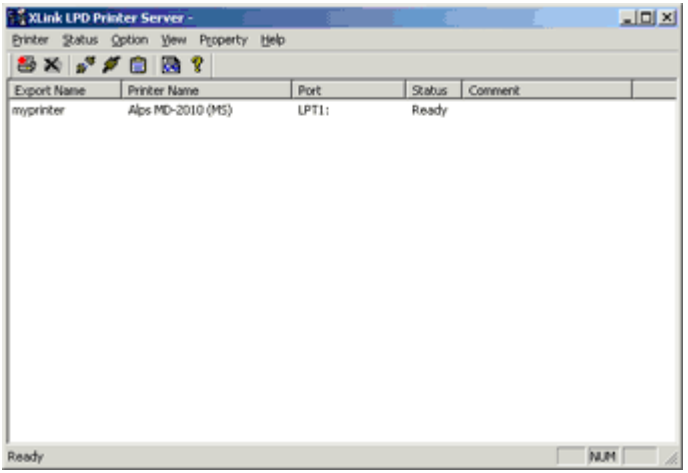
Post Script: Some printers may request post script formatting specifically. Select this one in the case.

Raw Format: This selection will keep the files original formatting without any modification.

Text Format: This selection can be used for general text files.

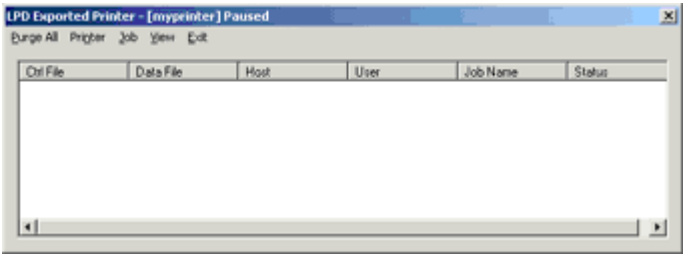
The 'Unix to DOS conversion' will replace the "end of line" mark in a unix file with a CR character so that when viewing from windows, the file will be properly lined up.

Click 'Finish' to close the dialog box. Now back in the user interface screen again. You will see the printer just defined with 'Status': Ready.



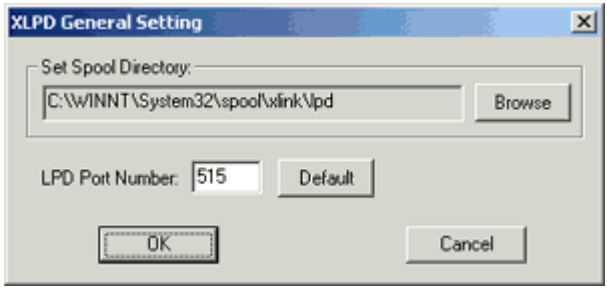
Viewing the queue

To see if a printing job is received by LPD server, you need to first 'Pause' the printer by click on 'Status/Pause' from the user interface screen. Then, you click on 'View/Queue' to open up the 'queue' screen as shown in following. Upon issuance of an 'lp' command, if all is working properly, you should see the job listed in the queue.



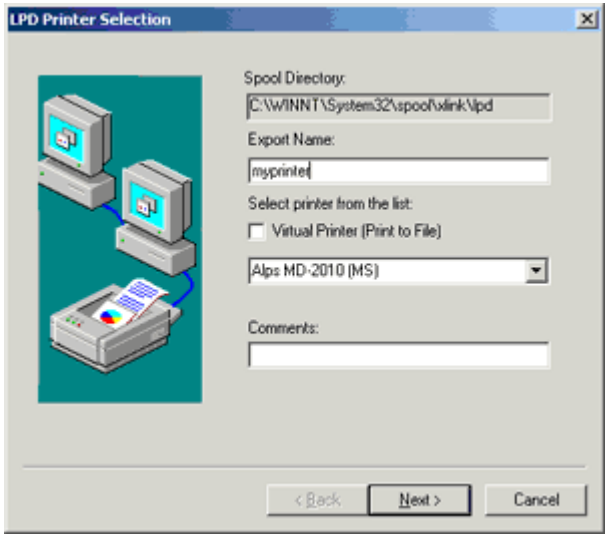
Change printer port

The standard printer port is 515. It is set as default for XLPD server. In case you need to change the port number, click on 'View/Setting' from XLPD user interface screen to bring up next dialog box. The port number can be changed by typing in the new number directly in the screen.



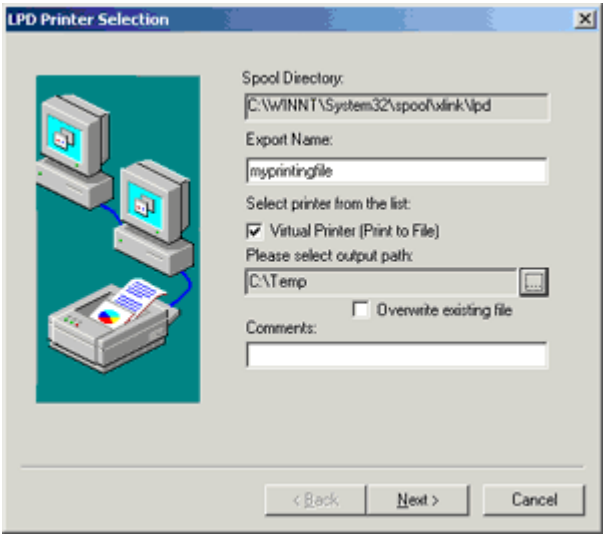
Edit a printer setting

If there is anything you need to change in the settings of an already defined printer, from XLPD user interface, click on the printer's name, then click on 'Property' to bring out the dialog box for making the changes.



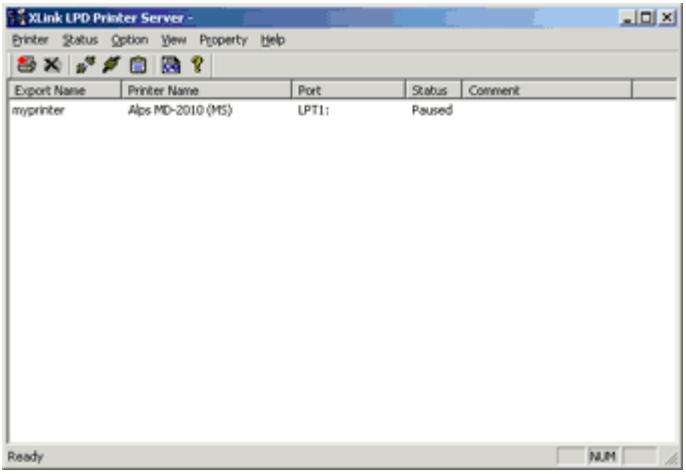
Print to a file

There are times that you want to save a printing job for later print. This is the situation we refer to as 'print to a file'. To print to a file, you click 'Printer/New' from XLPD user interface screen to open up the dialog box. Type in a name for the printer, then check the box 'Virtual Printer', and select the drive and folder where you want to save the file.



General Trouble Shooting

The general trouble shooting method is to help you narrow down the possible source of problem. Because XLPD server is like the "middle man" that sits between the print-requesting-system and the printer, the easiest way to go is to find out if the problem occurred before XLPD server received the printing job or after it.



So you first 'Pause' the printer (click on 'Status/Pause' from the user interface screen). Then, you issue a printing job from the client system. Take a look at the queue to see if the printing job is received.

Analysis:

If the printing job is listed in queue, it means both LPD and LPR are set and functioning correctly. Then if you can't get the file printed, check the printer driver, the printer connection (you may try to print a local file from the windows system and see if it will print) and other possible complications.

If the printing job is not listed in queue, it means either LPD or LPR (or both) is not properly configured. Or maybe there is a network connection problem between the systems.

CHAPTER 8

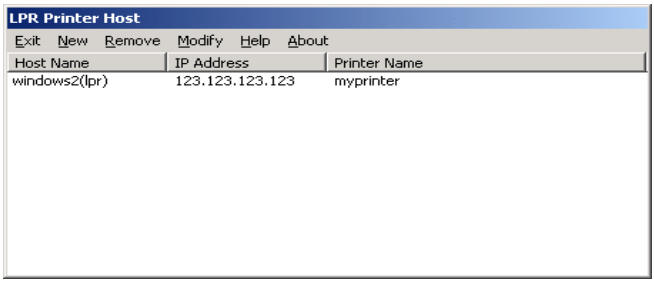
LPR Hosts

Introduction

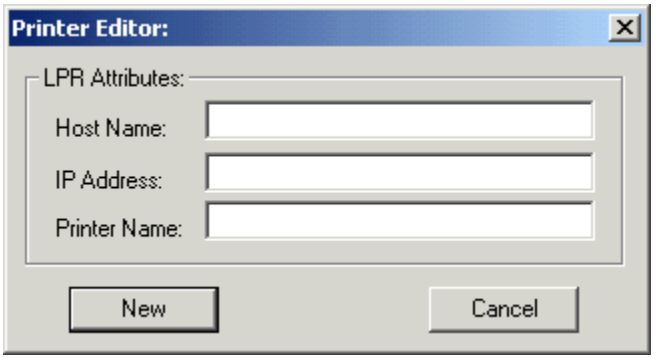
The **LPR Hosts** utility is used to define hosts running **LPD** as **LPR** printer servers. The purpose of this application is the same as the Host Editor. In order to add an **LPR** printer to a Windows operating system, it is required to run this utility first to create a list of hosts with remote LPR printers for Network Neighborhood on Windows systems.

Starting LPR Hosts

Click on the **LPR hosts** icon, the **LPR hosts** dialog box will show as following:



Click the **New** button to open up “Printer Editor” dialog box.



In this box, you enter (remote) Host Name, its IP Address and the Printer Name. You will see an entry like the one shown in above GUI when you finish define a new remote printer. Now an LPR printer server is inserted into an LPR host list.

You will then be able to add the LPR printer to your local system and set it as the default printer as if it is local to your system. For details on how to add an LPR printer to your local system, go to next chapter.

CHAPTER 9

Adding Network Printers

Introduction

Omni Print functions are seamlessly integrated with the Printer Manager on Windows platforms and supports both NFS and LPR printers. This chapter explains how to set up remote printers.

Setting Up and Using NFS Printer

To setup NFS printer, the remote UNIX stations or printer servers must have **PCNFSD** or **RPC.PCNFSD** running. Following are the details on how to add a NFS printer to your Windows systems.

Remote Printer Name

A printer name is a printer queue you have defined and exported on NFS servers or UNIX stations. Two important steps are needed on remote UNIX stations or NFS Servers before you are able to add a remote NFS printer to your Windows 95, Windows 98 or Windows 2000/NT/2003. First, you need to export the spool path, (e.g. "/usr/spool") from the UNIX system to the network. Second, you need to define a dumb printer or a printer queue with no filter on the UNIX system.

Example:
If HP712 is your NFS server and has a HP Laser Jet III connected to it, the first step is to export the spool path "/usr/spool", then define a printer name for HP printer on HP712 station. Please note that you MUST select a "dumb" driver for this printer name instead of HP Laser Jet III driver. Type the command "exportfs -a " to get the export list and command "lpstat -t" to get the printer name list.

*Special Note for SCO System***:**
If SCO System is your NFS server, you may need to set access permissions of the path '/usr/spool' so that it is opened to everyone by the command 'chmod 777 /usr/spool'.

Adding NFS Printer To a Windows system

On the Windows system,

Double click on **My Computer** icon

Double click **Printers** icon from **My Computer** window.

Click **Add Printer** icon from the **Printers** window.

Select **Next**

Select **Network Printer** in ADD PRINTER WIZARD box

Select **Next**

Click the **Browse** button.

Double click **Entire Network**

The dialog box will prompt you to enter the path and the name of a printer in the Printer field, or you can click **Browse** to select a printer from the Entire Network windows. For example**:**

Click **Browse**

Double click **Entire Network** icon

Select: **HP host**

Double click **Dumb1**

When the desired printer has been selected, click on **OK**. You may be prompted to select a driver for the printer if one is not currently installed on the network. The connected printer will appear as the default printer on the Printer Manager Toolbar.

Setting up and Using LPR Printer

In order to add a remote LPR printer to your Windows system, you need first to run **LPR hosts** to define some hosts running the LPD printer servers. Please refer to Chapter 8 - *LPR Hosts* for more details.

To Add LPR Printer to Windows systems:

Double Click **My Computer** icon
Double Click **Printers** icon
Double Click **Add Printer**
Click **Next**
Follow the steps of Add Printer Wizard and select **Network Printer**
Click **Next**
Click **Browse**
Double click **Entire Network** to get hosts list
Select a host printer with **lpr** extension

e.g. hp(lpr)

Continue on to complete the printer adding process until you see a new printer icon showing in the printer group.

Troubleshooting

- ***Why can't I print after I add the printer to my system?***
  There is always a chance that your print job may not behave as expected. You will need to see if:
  - TCP/IP connection is set up properly
  - PCNFSD is running if you are using NFS printer
  - LPD is running if you are using LPR Printer
  - Spool directory is accessible
  - Correct filtering option is set
  - Correct printer path is defined

- ***Why do I get errors if I try to define a network printer under Win NT?***
  In Windows 2000/NT, even if you browse the printer path, it might only show the printer name. If this is the case, you need to manually add the full path before the printer name.

  For Example:
  If the printer is defined as hp5p on an HP1000 (UNIX server name), Windows 2000/NT will only show 'hp5p' as the printer location. You will need to add the following line; \\HP1000\hp5p for the printer to be validated properly into your Windows 2000/NT system.

CHAPTER 10

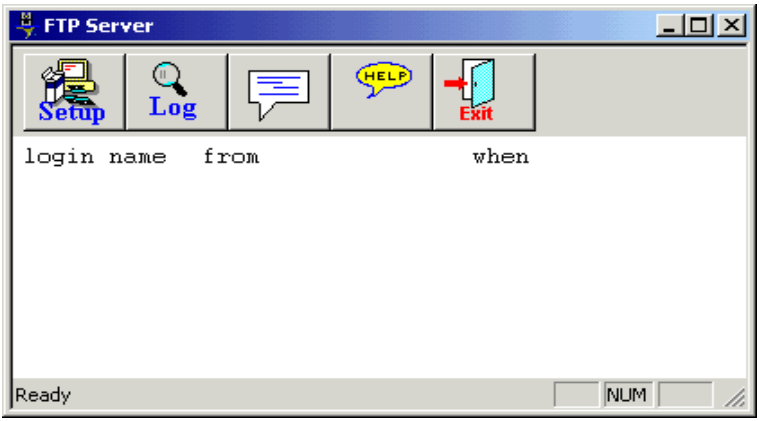
FTP Server

Introduction

FTP server utility allows you to configure a Windows system to become an FTP server. It provides tools to set up user accounts with assignments to the home directory, as well as individual access permissions.

Starting FTP Server

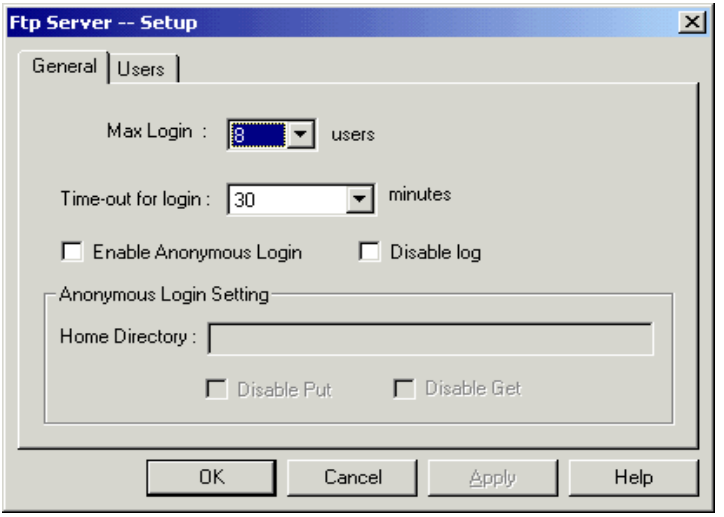
To start the FTP Server, double-click the FTPD icon in the OMNI-NFS series program group. An FTP Server dialog box will appear.



The FTP server Log allows you to check on the connectivity history of the FTP server. All user connections will be dropped with exiting of FTP server. So, before you Exit FTP server, make sure there are no users connected at the time.

Configure FTP server

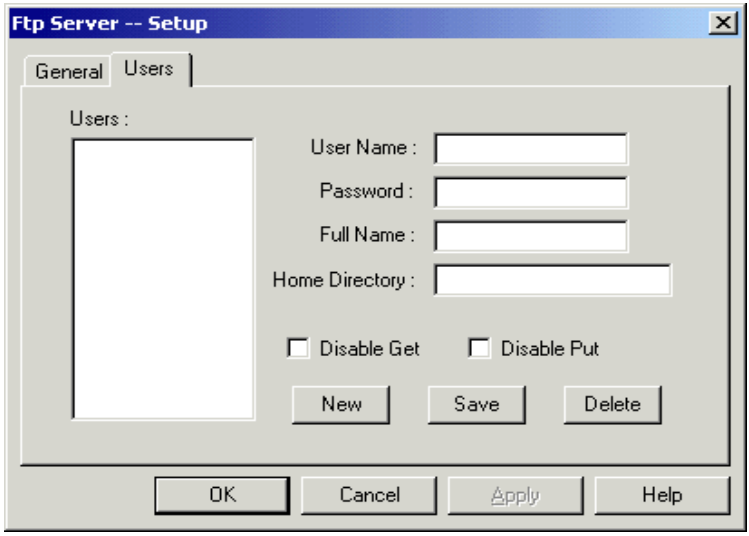
Click Setup button to set the number of users and time-out length of time for the FTP server.



The default number for Max Login (concurrent connection) is set to 8. If the number of users logged in exceeds the set number, the subsequent connection to the FTP Server will be refused and closed. For example: with above setting, at any time when there are already 8 connections established through the FTP server, the 9th connection will be terminated right after login. Omni FTP server allows maximum of 16 concurrent connections at any time.

If a user's idle time exceeds the pre-set time-out length of time, the FTP connection will be terminated.

Click Users button to enter users' information.



FTP client's account name, password and home directory are required for each user connection. If no password is assigned, user login will fail. Click 'Save' after entering a user's information. Click 'New' to start creating next account. Click 'Delete' to remove an existing account. It is convenient to setup all users' account that may need to access the FTP server.

'Disable Get' will restrict download information by the FTP client from the server. 'Disable Put' will restrict the FTP client to upload information to the server.

CHAPTER 11

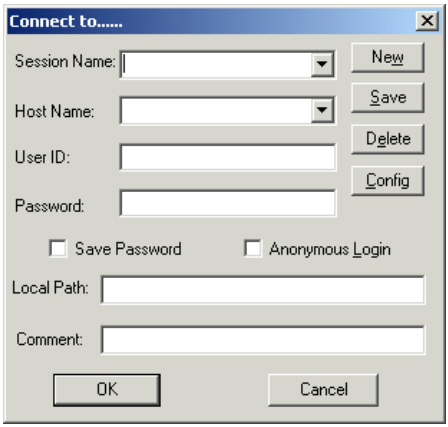
FTP Client

Introduction

Omni FTP client is used to provide file transfer services across a wide variety of systems through the use of the File Transfer Protocol (FTP). It enables users to copy files and directories from one system to another. Simple types of files such as an ASCII text or a sequence of binary data records can be transferred through FTP connection. This connection also allows users perform remote file system control such as listing files, changing directories, and switching local drives.

Using FTP Client

Using FTP client to transfer files to and from FTP servers, click on the FTP client icon in an XLink program group.



Start by selecting the session configuration from the dropdown menu or create a new session name, then select(or enter) a host name or IP address.

Enter the user name and password for the remote FTP system. You also have the option to save the password for future connections. For anonymous login, check on the “Anonymous Login” box. You can assign a local directory as the default directory after you successfully connect to the remote FTP server.

After login, user is able to:

- Transfer files and directories between local and remote systems.
- Delete files on a local or remote system.
- Rename the file on a local or remote system.
- View the file on a local or remote system.
- Make new directories on a local or remote system.

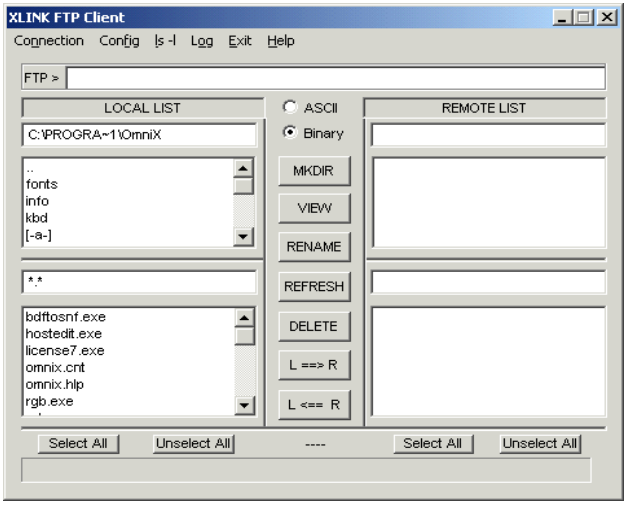
There are also commands that enable the user to:

- Connect and disconnect from the remote system.
- Configure the viewer functions.
- List all the files on a remote system.
- Display the login status message.
- Identify whether ASCII text or binary data is to be transferred.

All transfers are executed in either ASCII (text) or binary mode. ASCII mode performs carriage return/line feed translation and is only needed when transferring text files for use on a non-Windows system.

Note: If an anonymous user is defined, connection attempts for "anonymous" are accepted, regardless of the defined password or the password supplied in the pop up windows.

The FTP Windows allows you to connect and disconnect from the remote host, transfer files between local and remote systems, and view the contents of a file. The following is the description of these functions.

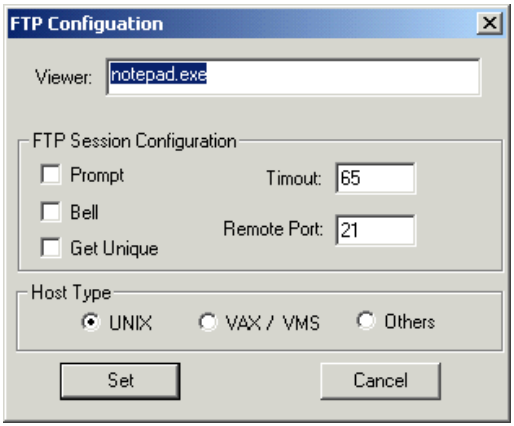


"Connection" Menu

This menu allows you to connect and disconnect from the remote host you select.

"Config" Menu

This field allows you to select the Edit program utilized to view the file. The default is Notepad.



The FTP Configuration includes the following options:

- Prompt: If you select this option, you will get a prompt dialog box before you send or receive files.
- Bell: This option enables bell sound if any error occurs.
- Time Out: The maximum time allowed to establish a connection.
- Remote Port: You can set the port number in this field.

The host type field includes three options, you can choose one of them.

- UNIX
- VAX/VMS
- Others

"ls –l" Menu

This menu will show the details of the file list on the current directory of the remote host.

"Log" Menu

This menu shows you the details of login and transfer status.

"Exit" Menu

Press this button to close the FTP application.

The **"ASCII"** Button

Check this box while you perform carriage return/line feed translation and transfer text files for use on a non-Windows system.

The **"Binary"** Button

Select binary mode for transferring binary raw files.

The **"MkDir"** Button

To make a new directory on a local or a remote system, you simply select the parent drive and directory and press the MkDir button. After pressing this button, the dialog box will prompt you to enter the new directory name.

The **"Delete"** Button

To delete files on a local or a remote system, highlight the files you wish to delete, then press the "**Delete**" button. The files you have highlighted will be deleted.

The **"Rename"** Button

To rename the file on a local or a remote system, highlight the file you wish to rename, on the local drive or on the remote system, then press the "**Rename**" button. A dialog box will prompt you to enter the new file name.

The **"View"** Button

To view the file on a local or a remote system, highlight the file either on the local drive or on the remote system, and press the "**View**" button. The dialog box will show the content of the file you want to view. The default viewer/editor program is Windows Notepad.

The **"L===>R"** Button & The **"L<===R"** Button

To transfer files between local and remote systems, highlight the files or directories you wish to transfer, then press the arrow button. The files you have highlighted will be transferred to the other system, into the directory currently displayed. You can also select this transfer command from the Commands menu bar.

Troubleshooting

- ***If you experience difficulties in using the FTP application, check the following items:***
  - Verify that installation and setup has been successfully completed.
  - Make sure the remote system provides an FTP server and that it is running. Note that some operating systems do not supply TCP/IP services with the standard package (for example, VMS).
  - If the FTP application reports a failure to connect error message, use the Ping application to verify that the connection to the remote system is working.
  - If the FTP application reports a failure to login, verify that the user name and password were entered correctly.
  - Make sure the correct transfer type (ASCII/binary) is chosen correctly. Transferring a binary file when the transfer type specifies ASCII may cause a failure in transfer.
  - Make sure you have permission for specific operations (for example, write access to a directory).

CHAPTER 12

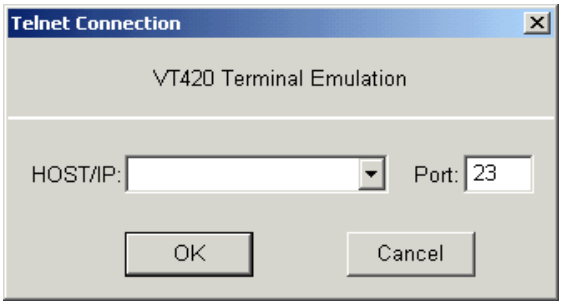
VT420 (Telnet)

Introduction

Omni VT420 is a terminal emulation program. With added features, such as keyboard mapping, background/foreground color selection and personal control of many general system settings, Omni VT420 has become a useful tool one enjoys using while getting work done.

Using VT420 Terminal Emulation

VT420 is a terminal emulation program that allows you to connect and communicate with hosts that support VT100, VT220, VT320, and VT420 terminal modes.



Multiple Session Capability

You can start more than one session at a time and use VT420 to open multiple Telnet windows on a single host or a group of different hosts. You can also create custom icons using the "Program Manager " which allows you to click on the icon to directly start your VT420 session.

Starting and Terminating VT420

To start a VT420 session, follow the steps below:

1. setup Host Editor (see chapter 6)
2. start VT420 by double clicking on the VT420 icon in the Omni-NFS Program Group
3. a “Connect Host” dialog box will appear, you select the host from the drop down menu
4. click “OK”

Once you have connected to a host, the VT420 window will appear on your display. The host name you specified will appear at the top of the VT420 window, and the host login prompt will appear in the window.

Enter the login info required for your host system. Once the connection is established, the VT420 window will appear active on your display. You can interact with the host by choosing commands from the displayed menus, or by typing commands in the VT420 window.

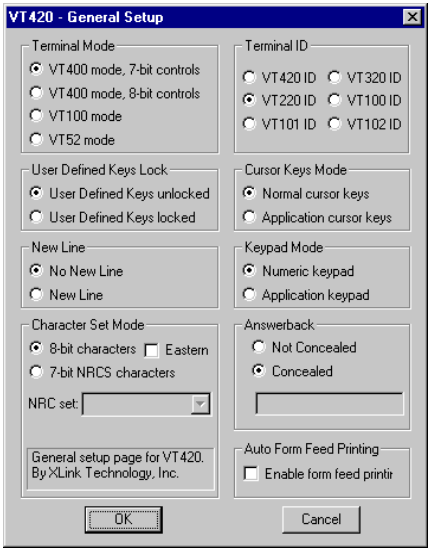
To terminate a VT420 session, you double click on the "close" icon of the Control Menu box, or by selecting **Exit** from the Telnet **Commands** menu.

In the connected VT420 windows, a “Setup” button is there for you to manipulate the settings of the connection. Following are the detailed explanations on items in “Setup”.

General Setup

This General Setup menu item allows you to choose the terminal and cursor type, UDK, or keypad. (see picture in next page)

Here is a list of General Setup items available:



Terminal Mode

VT400 mode, 7 bit controls

Lets the terminal uses all available VT420 features. The terminal normally uses 8-bit graphic characters and 7-bit control characters. You can also select this mode for VT200 and VT300 applications. This mode is recommended for most applications.

VT400 mode, 8 bit controls

Lets the terminal use all available VT420 features. The terminal uses 8-bit control characters. If your application uses 8-bit control characters, you must select this mode.

VT100 mode
This mode lets the terminal operate as a VT100 terminal. Use this mode for applications that require VT100 compatibility.

VT52 mode
Lets the terminal support VT52 applications. VT52 mode is not compatible with VT100 and VT400 modes.
The default terminal mode is VT400 mode, 7 bit controls.

Terminal ID
The terminal emulator can report to the remote host as different terminal types. If your operating system or application programs on the remote host need (or only supports) specified types of terminals, you may change the Terminal ID parameter to fit the requirement.

In ANSI modes (VT100 or VT400 mode), you may set the terminal ID to VT420, VT320, VT220, VT102, VT101 or VT100 ID. In VT52 mode, the terminal only has VT52 ID.
The default terminal ID is VT220 ID.

Users Define Keys Lock
The User Denied Keys (UDK) can be changed or not changed by the remote host. If UDK is locked, the remote host can not change the definition of UDKs. You may change the UDK definitions locally. See User Defined Keys Setup.
The default value of this parameter is UDK unlocked.

Cursor Keys Mode
Cursor keys act in two modes: Normal cursor mode and Application cursor mode. The cursor keys send different codes to the remote host depending on the cursor mode. Normally, you don't need to change this parameter. It may be changed by control codes of the remote host.
The default cursor mode is Normal cursor keys.

New Line

If the parameter of "No New Line" is selected, the terminal will only send the **Carriage Return (CR)** code to the remote host when you press **ENTER** key. Otherwise, it will send both Line Feed (LF) and CR code to the remote host in "New Line" mode. The default value of this parameter is "No New Line".

Keypad Mode

Keypad mode acts in two ways: Numeric mode and Application mode. Normally you don't need to change this mode setting. It may be changed by control codes of the remote host.
The default keypad mode is Numeric mode.

Character Set Mode

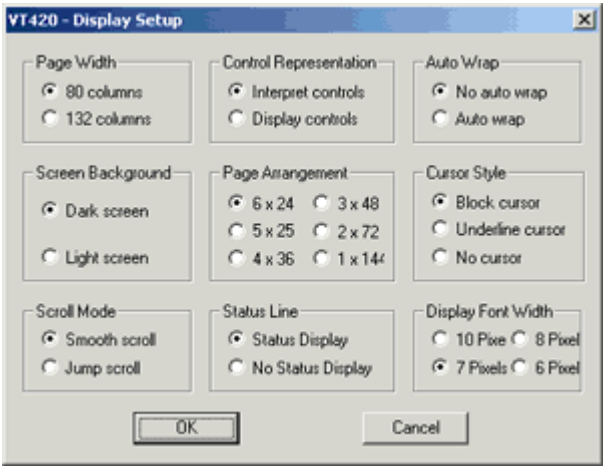
Allows you to set characters to either 7 bits or 8 bits.

Answerback

The Answerback message Specifies a sequence of characters that are sent to the host when ^E (Control E) char is received.
If **Not Conceal** is set, then the terminal will display the answerback message.

Display Setup

This Display Setup menu item allows the user to adjust the terminal page width, screen background, cursor style, and scrolling method. Here is a list of Display Setup options available;



Page Width

The width of the terminal can be set to 80 columns or 132 columns. If you change the width of the page, the display of the current terminal screen will be erased.
The default page width is 80 columns.

Control Representation

The terminal emulator can display, interpret, and then execute the control code when receiving a control codes from the remote host. When you select the display control mode, all control codes will be displayed using a special font. This is usually used for debugging.

Auto Wrap

Auto Wrap allows to you to select whether or not the text will automatically wrap to the next line when you reach the right margin.

No Auto Wrap
This feature lets the terminal display each new character in the last column of the line when you reach the margin. Each character will overwrite the previous character at that position.

Auto Wrap
This feature lets the terminal display the new character on the next line when you reach the margin. By default, the terminal does not invoke the auto-wrapping mode.

Screen Background
This feature allows you to select light text on a dark background, or dark text on a light background. The default screen background is the Dark Background.

Page Arrangement
This feature allows you to select the number of lines per page. The following modes are supported.

6x24, 5x25, 4x36, 3x48, 2x72, or 1x144.

The default page arrangement is 6x24 lines.

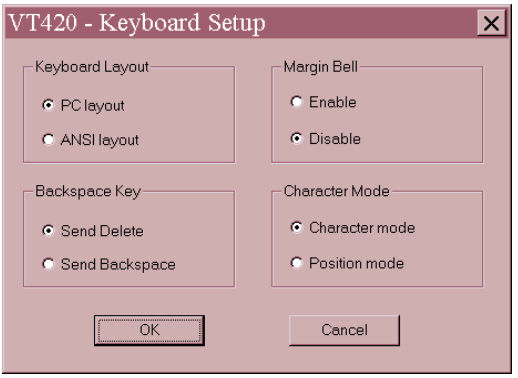
Cursor Style
This feature allows you to enable or disable the cursor. You can also select block or underline cursor when the cursor is enabled.

Scroll Mode

Smooth Scroll
Selection of this mode sets the screen scroll whenever it detects a scroll request. This is the default scroll mode.

Jump Scroll
Selection of this mode prevents the terminal from scrolling until there are no longer any characters received. This mode makes the terminal scroll at a faster rate.

Keyboard Setup



Keyboard Layout

PC Layout

Allows you to use the PC keyboard definition for sending key codes to the remote host.

ANSI Layout

Allows you to use ANSI keyboard definition when sending key codes to the remote host. This layout is convenient for you if you are familiar with the ANSI keyboard layout.

Margin Bell

Allows you to enable or disable the margin bell. If the margin bell is enabled, the speaker will sound when the cursor is eight characters from the right margin.
By default, the margin bell is disabled.

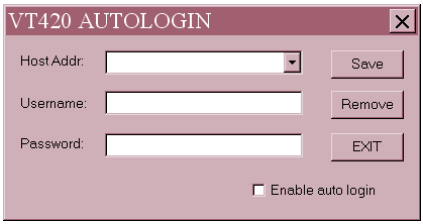
Backspace Key

Allows Backspace key to send a Delete code. Some applications require the Backspace key to send a Delete code. In such case, change this parameter to fit the application you are running.
By default, the Backspace key will send the Delete code.

Character Mode
Allows the user to select the keyboard operating mode.

Auto Login

Auto Login enables the user to predefine the user name and password to a specific Host listed in the Host Editor. Users can now login without having to manually type in his/her User Name and Password. It is designed to simplify tasks for users with multiple UNIX accounts and different identities.



Host Addr
The default host addresses contained in this list are the host addresses defined in the host database (using Host Editor). User can also manually type in other IP addresses or domain names in the editable area.

Username
Enter user login name for the selected Host Address.

Password
Enter login password for the selected Host Address

Enable Auto Login
This option enables/disables the auto login function for a specific Host Address.

Printer Setup

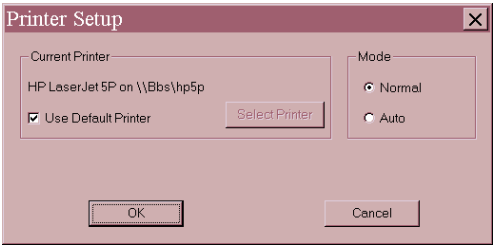
Select the Printer button to see the Printer Setup dialog box. In this dialog, you can designate the output device for your printer setup. The Printer Setup dialog contains the following options:

Normal

This option sends no output to the printer. This is the default.

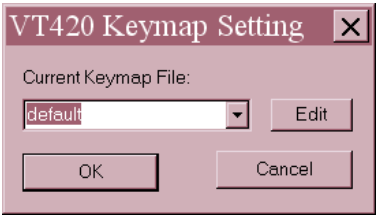
Auto

This option sends the current line of text to the printer when the terminal receives a line feed character. This mode is most useful when the printer is operating in scrolling mode; it does not work well in full-screen mode. This mode may be toggled on and off by the user as well as by the host software.



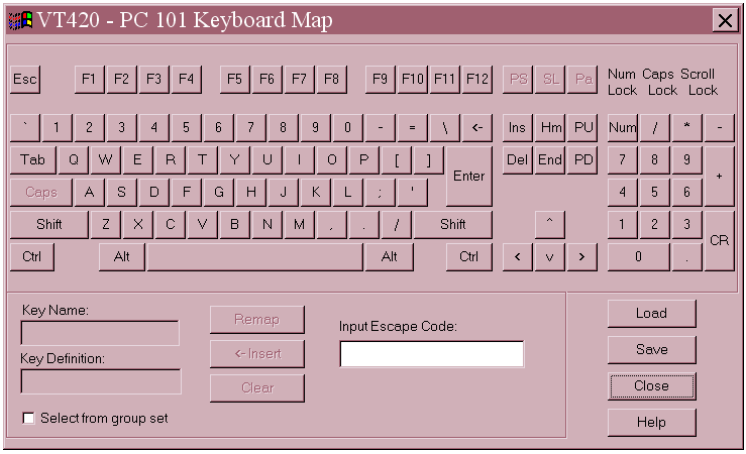
Keymap

VT420 also provides keyboard re-mapping utilities on the VT420 sub-menu which allows you to select XLink predefined keymap files or create your own key definitions.

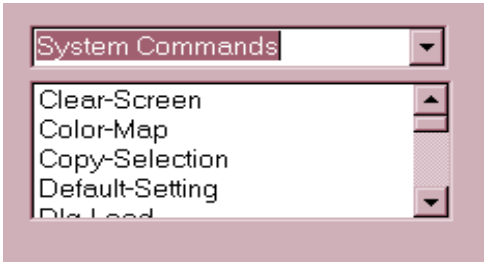


Keymap files can be modified by selecting a file from the list followed by clicking **Edit.** Keyboard settings are applied immediately after selection.

By clicking on the **Edit** button, a keyboard layout will be displayed for the user to modify any key definitions.



User can either specify the **escape code** or selecte from the list by checking the **Select from group set** box as shown below.



Follow these steps to define a key:

1. Select a key by pressing the key buttons on the keyboard layout; (Key name will display the key button that is selected for modification).

2. Click on the **Remap** button and input the key definition in the **text box** or **select from group set** followed by pressing the **Insert** button. (**Remap** button is changed to **OK** button)

3. Click **OK** button to finish the mapping.

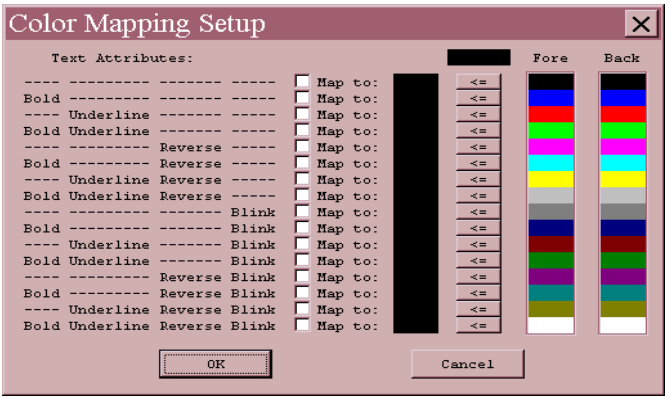
4. After all the key definitions are completed, the user can click on the **Save** button to save the keymap file (all keymap files have the extention .kmp); otherwise, the modification will be discarded upon exiting VT420 or re-editing of the current keymap.

Color Mapping Setup

You can simulate host session color schemes or create your own window colors by using the Color Mapping Setup.
Within this dialog box you can choose preset color schemes, make your own, or assign specific colors only to specific character attributes. A number of preset color schemes are available for you to choose from. These color schemes include colors for text attributes and background.

Assigning colors to individual text attributes

You can assign any color shown on the available color palette to any one of the text attributes or to the screen background.


Color Mapping Setup
Text Attributes:
Fore
Back
---- --------- ------- ----- Map to: <=
Bold --------- ------- ----- Map to: <=
---- Underline ------- ----- Map to: <=
Bold Underline ------- ----- Map to: <=
---- --------- Reverse ----- Map to: <=
Bold --------- Reverse ----- Map to: <=
---- Underline Reverse ----- Map to: <=
Bold Underline Reverse ----- Map to: <=
---- --------- ------- Blink Map to: <=
Bold --------- ------- Blink Map to: <=
---- Underline ------- Blink Map to: <=
Bold Underline ------- Blink Map to: <=
---- --------- Reverse Blink Map to: <=
Bold --------- Reverse Blink Map to: <=
---- Underline Reverse Blink Map to: <=
Bold Underline Reverse Blink Map to: <=
OK
Cancel

Troubleshooting

- ***If you are starting up a VT420 and the VT420 window isn't created, check the following list:***

  1. Verify the host is up and running.

  2. Verify the host name or IP address you entered. If you specified a host name that didn't work, specify its IP address instead.

  Addresses are specified in dot notation as follows:

  value.value.value.value

  Each value must be in the range of 0 through 225. Values starting with **0x** or **0X** are treated as hexadecimal. Values starting with **0** are treated as octal. All other values are treated as decimal.

  If this format works and entering a host name doesn't, then somewhere in the network your host name is not being translated to the correct address.

  If your transport resolves the host names with a hosts file, you can view and edit this file from the **Host Editor**. If your transport uses a different method to translate host names to addresses, consult your transport documentation.

  3. Ask your network administrator if the Telnet daemon is up on the host. Sometimes it is not running.

  4. Lastly, confirm that your host supports Telnet. Some hosts do not.

CHAPTER 13

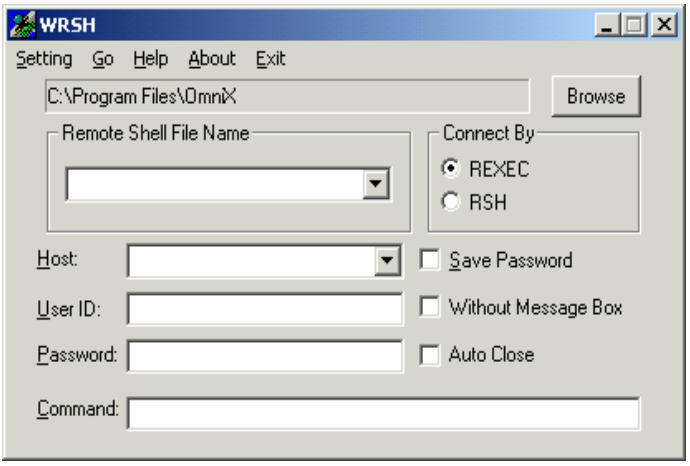
RSH (REMOTE SHELL)

Introduction

The RSH application allows you to execute commands on the remote host without having to login first. To use RSH, your machine may need an entry in the **.rhost** file in your home directory on the remote host, depending on the UNIX system.

Using RSH

When you run the RSH application, you will get a **Remote Shell** dialog box:



In the dialog box, you must specify the **Host** to which you wish to connect, and your **User Id** and **Password** for the host. The Host name can be selected form the drop down box. The **Command** you wish to execute must be a UNIX command native to the particular UNIX host.

e.g. # ls –l (current directory listing)

 # pwd (show current path)

You can save the current settings as default. After you have provided all the information that the RSH application needs, you can click on the **GO** button to execute the command.

Without Message Box

Check this box if you wish to disables any message box that informs users the status of the command.

Auto Close

Enables users to terminate RSH application right after the execution of commands.

Note: Only one simple command can be performed each time. The RSH files can also be run as script files to execute simple commands form your desktop.

APPENDIX A

NETWORK LOCK MANAGER (NLM File Locking)

The Network Lock Manager (NLM) is an RPC service that provides advisory locking of files across the network. There are various versions of the NLM in existence; this implementation is version 3.
Because the NFS protocol is stateless and has no knowledge of locks that may or may not have been granted, clients that wish exclusive access to a particular file must call the Network Lock Manager on the server to request access. The server Network Lock Manager is responsible for creating and destroying locks on files, as well as mediating requests for shared or exclusive file access.
This version 3 implementation supports file locking and sharing for DOS machines under **Windows 95/98** and **Windows 2000/NT** on the net.
File sharing is a mechanism which allows a DOS process to open or create a file and to restrict the way in which subsequent processes may access the file. For example, a DOS client may request that a file be opened for reading and writing, and that subsequence users may only open it for reading.
File locking is a mechanism that only allows one DOS process to open or create a file using the same name in the same location at the same time. For example, a DOS client may request that a file be opened for reading and writing, and the subsequence users can not open it.

File Locking

All the files in this mounted drive will follow File Locking mechanism while File Locking is selected. For example, if a DOS NFS client with **File Locking** has already opened a certain file, then another NFS client with **File Locking** can not open the same file simultaneously.

No Locking

All the files in this mounted drive will *not* follow the File Locking mechanism while No Locking is selected. For example, a DOS NFS client with **No Locking** can open any files for reading and writing no matter which file is opened whether it is dedicated to be locking or no locking.

Read Only

All the files in this mounted drive can only be opened for reading and not for writing when **Read Only** is selected. For example, a DOS NFS client with **Read Only** can only open files for reading no matter which file is opened by locking or no locking.

APPENDIX B

PCNFSD

PCNFSD Protocol Definition

The purpose of the PCNFSD protocol is to provide a personal computer NFS client with the authentication and network printing services that are usually available in larger and more capable systems. It use, while not necessary, is highly desirable. The source code for the server implementation of PCNFSD is freely available from Sun Microsystems.

Authentication

The NFS file access control model is based upon the uid/gid mechanism used in X/Open-compliant systems. All NFS remote procedure calls must be made with AUTH_UNIX credentials from which a uid and gid can be extracted. If a client implementation supports the use of NFS services without any form of authentication, it should use the uid/gid pair (0xfffffffe, 0xfffffffe) (i.e., (-2,-2)), which is conventionally associated with the identity “nobody”. Client and server support for access as “nobody” is an implementation or administrative option.
Operation as “nobody”, while feasible, is undesirable, since the client can only access file system hierarchies with unlimited “other” permissions, and administrators of server systems have no way of controlling resource usage. For this reason, it is expected that personal computer NFS implementations will require or encourage users to establish valid access credentials. A typical implementations might be to prompt the user to enter a username and password, which could then be validated using the PCNFSD_AUTH procedure, which will return a uid/gid pair. The client can then use this information to synthesize the AUTH_UNIX credentials for subsequent RPC requests.
Since it is undesirable to pass clear-text passwords over a network, both the username and the password are mildly scrambled using a simple exclusive-or operation. The intent is not to be secure but to defeat “browsers”.

Print Spooling

The availability of NFS file operations simplifies the print spooling mechanism. The PCNFSD returns the name of a directory on the server which is exported via NFS and in which the client may create spool files. It also accepts start-print request from the client.

APPENDIX C

How to setup LPR on remote Unix systems

Listed below are examples of how to setup LPR on remote Unix system on four kinds of Unix systems.

1. Sco UnixWare

   Open “Sco Admin” dialog box, select “Printer Setup Manager”

   Select ‘printer => ‘Add TCP/IP printer’

   a) name – give a name you want to call the printer

   b) Portocol Type – lpd

   c) Make/model – select the matching one

   d) Printer connection type – select “on remote server”

   e) Remote system – select or type the remote server system

   f) Remote Printer – the name defined in XLPD

2. HPUX

   #sam

   select ‘Printer/Plotters’ => actions => add remote printer/plotter

   a) printer name – give a name you want to call the printer

   b) remote system name – can be either the remote system name or its IP address

   c) remote printer name – the printer name defined in XLPD

3. Linux

   From KDE drop-down menu, select KDE menus => system =>

   KDE control panel => Printer

   Click on “New” in the ‘Printer’ dialog box

   a) Queue name – give a name you want to call the printer

   b) Queue Type – select ‘windows printer’ or ‘Novell Printer’

   c) Select the match printer model

4. IBM

   #smit

   Select Print Spooling => Add a Printer Queue => Remote

   => Standard Processing

   a) name of queue to add – give a name you want to call the printer

   b) Host name of remote server – type in the remote windows system where XLPD is defined

   c) Name of queue on Remote server – type in the printer name defined in XLPD

APPENDIX D

Examples on how to start NFS server on a Unix system

Five examples on four kinds of Unix operating systems are listed below. First login as "root", then follow the steps to get NFS server service started.

1. **HPUX**
    a) sam (open up System Admin Manager) <RT>
    b) select Networking/Communications
    c) select Networked File System (FNS)
    d) select Local Directories Exported
    e) click on "Actions", then select Enable NFS Server
2. **IBM AIX**
    a) #smit <RT>
    b) select Communications Applications & Services
    c) select NFS
    d) select Network File System (NFS)
    e) select Start NFS
3. **Linux**
    a) #cd /usr/sbin <RT>
    b) #rpc.mountd& <RT>
    c) #rpc.nfsd& <RT>

    OR

    #/etc/rc.d/init.d/nfs start/stop <RT>

4. Solaris

a) #cd /usr/lib/nfs

b) #./nfsd&

c) #./mountd&

5. Sco UnixWare

a) #cd /usr/lib/nfs

b) #./nfsd&

c) #./mountd&

APPENDIX E

The system settings for cross domain file access with NFS server product

For Windows NT server

Assume domain A and domain B are set. Domain A is the trusted domain, and domain B is the trusting domain. Install Omni NFS Dual Gateway on domain A system.

1. on both domains, in 'User Manager/Trust Relationships', set the trust to the other domain

2. on domain B, in 'User Manager/User Rights Policy', add domain A's "Domain Admins" account to: 1) Access this computer from network; 2) Back up files and directories; 3) Restore files and directories; and 4) Take ownership of files or other objects

3. on domain A, go to windows 'services', stop service of Omni NFS server, click on 'startup' to open up the dialog box, in the section of "log on as", select "this account" and enter (or select from 'browse') local administrator account with its password

4. on domain B, share out all drives/folders your want the unix system (NFS client) to see, then you will be able to see them in domain A system and export them out from Dual Gateway/server gateway.

For Windows 2000 server

Please make sure following settings are set for the test:
1. assume: domain A and domain B systems, and Omni DGW is installed on the domain A
2. domain B is trusted to domain A, so that on domain A you have domain B trusted as "Tree Root" with "yes" for the "transitive" property
3. on domain A system, go to 'administrative tools/domain controller security policy', in 'security settings, select 'local policies/user rights assignment', then select:
   a) "Log on as a service" and add accounts: "Administrator" and "Domain Admins"
   b) "Restore files and directories", do the same
4. share out the folder needs to be seen by the unix on domain B system and defined it as a 'network drive' on domain A system
5. on domain A system, in windows 'services', select 'Omni NFS server', go to 'properties/log on', select 'this account', add "Administrator" account of domain B with its password

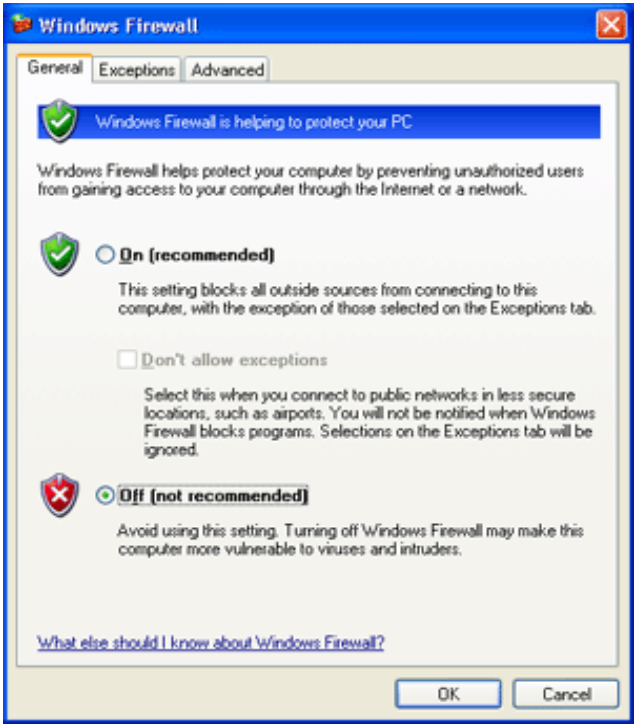
With all above settings done, you can now do the 'mapping' from Omni DGW where you can see domain B and its accounts. Then export the network drive shared from domain B, you can mount the exported drive from the unix system and access the files in it which are located in domain B system.

APPENDIX F

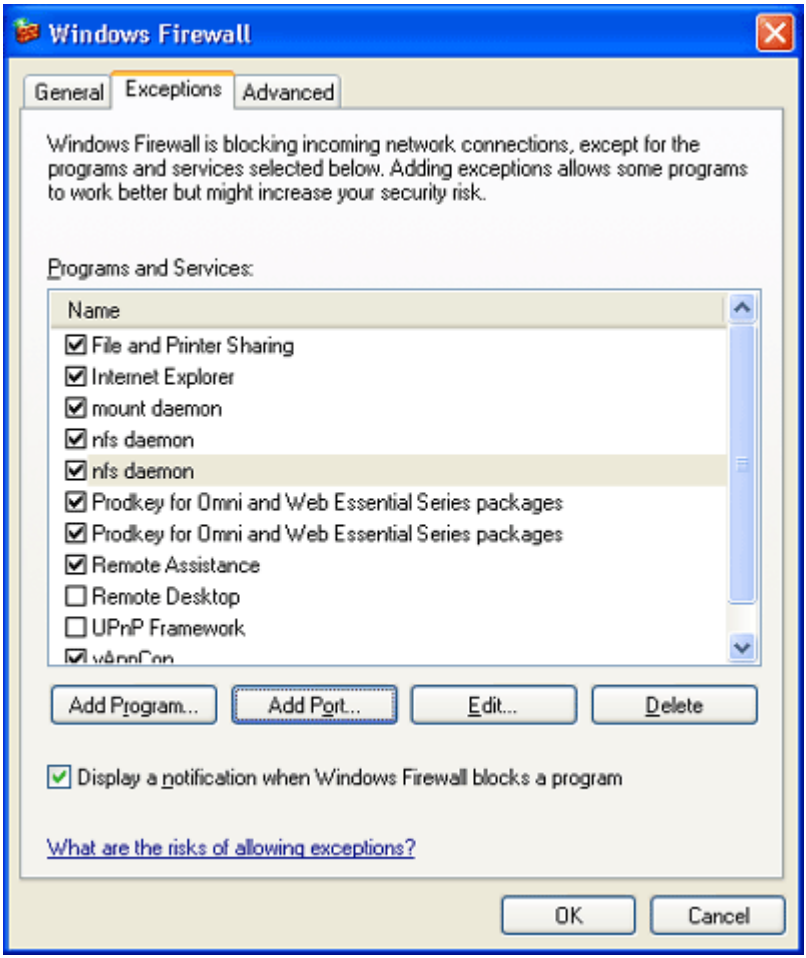
Firewall Setup on Windows XP and Vista systems

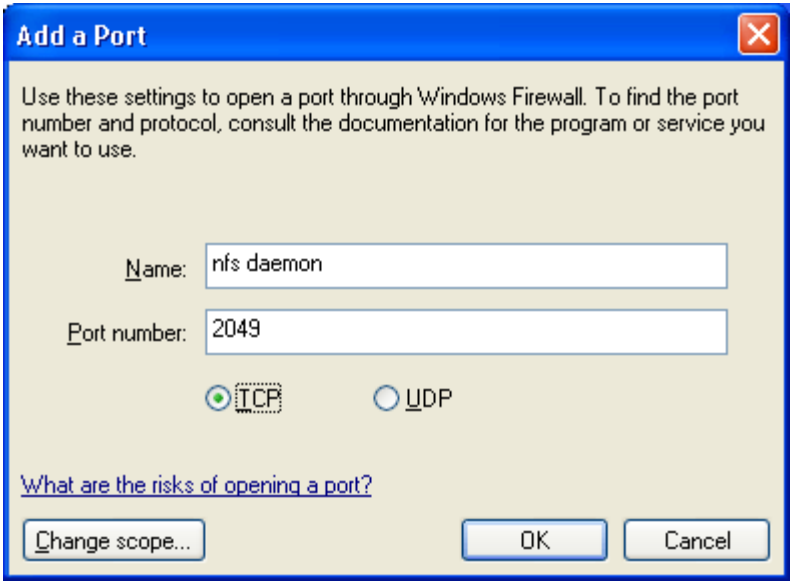
When running Omni NFS server on **Windows XP or Vista**, systems that have firewall included, it is important to configure the firewall to allow proper establishment of network connection.

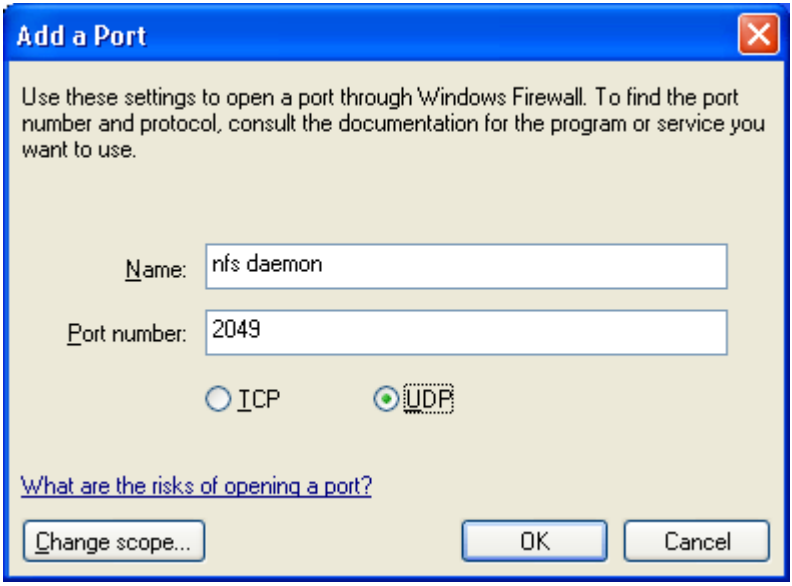
In general, if the NFS server and clients are part of an **intranet** system and firewall is not needed, the simplest way to configure it is to disable the firewall.


Windows Firewall
General
Exceptions
Advanced
Windows Firewall is helping to protect your PC
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
What else should I know about Windows Firewall?
OK
Cancel

If the firewall is needed, some TCP and UDP ports must be open to allow proper NFS connection. From Windows Firewall dialog box, select **Exceptions** and click **Add Port**




Add a Port
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Name:
nfs daemon
Port number:
2049
TCP
UDP
What are the risks of opening a port?
Change scope...
OK
Cancel


Add a Port
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Name:
nfs daemon
Port number:
2049
TCP
UDP
What are the risks of opening a port?
Change scope...
OK
Cancel

The two other ports to be added are :

1. mount daemon - 1058 (both TCP and UDP)
2. port mapper - 111 (both TCP and UDP)

If the firewall is still blocking the NFS connection with the above three ports open, additional ports may be opened:

1. For TCP connections
   - ports - 1030, 1031, 746, 747

2. For UDP connections
   - Besides all listed above, port 8 is also needed to be open.

GLOSSARY

Active Window

Also known as the focus window. This is the window currently accepting input. The mouse cursor must be in the window to make it active, and you may need to click on the window to make it active. If you can not see the cursor, you can generally tell which window is active because its border is highlighted. However, this depends on what window manager you are using.

Address

A number that identifies a unique location in the computer's memory where information is stored.

Address Resolution Protocol (ARP)

A protocol that translates Internet addresses into Ethernet addresses.

ANSI

American National Standards Institute

Application Clients

Application programs that run under the X-Window system.

ARP

Address Resolution Protocol

ASCII

Acronym for American Standard Code for Information Interchange. A standard set of characters used in data transmission applications.

AUI

Attachment Unit Interface. Interface type for Ethernet.

Baud Rate

The number of binary digits transmitted per second over a serial line.

Bitmap

A highly structured file that contains not only an image's picture elements or pixels, but also the type, sizes and color information.

Broadcast Address

The address used to send information to all equipment on the network.

Control Characters

Characters that send a command to the terminal when you type them, rather than sending the character itself to the screen display.

Data Bits

The number of bits in a transmitted or received byte of data (usually either 7 or 8). The number of data bits needs to be determined when setting serial communications parameters.

Default

A value or instruction in effect unless explicitly changed.

Download

Transferring data from a host to a terminal.

Ethernet

A local area network technology that uses Coaxial or Twisted Pair cable to interconnect different computers.

Ethernet Address

An address identifying a module on an Ethernet network.

Ethernet Driver

A program that receives and de-multiplexes the various packet types available over the network.

File Server

A computer on the network that provides services to client computers on the network. File servers often contain large amounts of storage and many software applications that can be used by multiple users at the same time.

Firmware

Software that resides in the computer's read-only memory (ROM). It generally controls the operation of terminals, printers and other devices.

Flow Control

A software-determined method for controlling the rate at which data is transmitted. Flow control is mainly used to avoid network congestion.

Font

A collection of characters and symbols that share a common design.

Font Directory/Path

The directory on the host where the fonts are located.

Gateway Machine

The computer that serves as a link between two networks.

Gateway Address

The Internet address of the gateway machine for the network. This is important when dealing with multiple networks, so that applications know if a machine is on a local network or on a network connected by a gateway machine. If networks are connected by a gateway machine, the gateway machine's address is included in the routing information.

Graphical User Interface (GUI)

Describes both the appearance and the function of window components (such as frames and canvases) and control items (such as buttons, pull down menus, and slide bars).

Host

The computer that provides application programs and fonts to the terminal.

Host Address

The unique Internet address of a host machine on the network. This address must be different from that of any other machine on the network.

Internet Address

Address of a node on the network using the Internet.

Internet Protocol (IP)

The Internet standard protocol that defines the Internet "datagram" as the unit of information passed across the network.

Modem

Abbreviation for Modulator/Demodulator. A device that converts digital data from a device into an analog signal that can be transmitted on a phone line. It also converts the analog signal received back into digital for the device.

Network File System (NFS)

A method of accessing files over a network on a host machine. The files look like they are in a directory on your machine, and you can use them as though they were your own files (if the permissions are set properly).

Network

Two or more computers connected by cable that use communication software to exchange information.

Network Address

A 32-bit-wide address divided into four 8-bit fields, that uniquely identifies a machine on the network. Each field is separated by a period. For example: 192.2.1.24.
The three basic types of address, Class A, Class B, and Class C are characterized as follows:

Class A	Used for large networks. A value from 0 to 127 in the first 8-bit field identifies the network as Class A. The remaining 3 fields establish the host address.
Class B	Used for medium-sized networks. A value from 128 to 191 in the first 8-bit field identifies the network as Class B. The first two 8-bit fields indicate the network address, the last two 8-bit fields establish the host address.
Class C	Used for small networks. A value from 192 to 255 in the first 8-bit field identifies the network as Class C. The first three 8-bit fields address the network, the last 8-bit field establishes the host address.

Packet

A set of information of a certain size sent between on a network. Packets have specific destinations, as opposed to datagrams which have no specific destination.

Path

A location of a directory on a computer, usually shown as a list of directories and subdirectories separated by a delimiter. A relative path is a list of directories that stand between your directory and the file you want. An absolute path is the path starting from the root directory (/). Note that the path does not include file names.
For example:

Absolute path:	/home/xlink/usr1/misc.	
Relative path	(if you are in "xlink"):	usr1/misc.

Protocol

The set of language rules that two networked machines must follow in order to communicate.

RAM

Random Access Memory. Memory chips that can be written to or read from. Data stored in these chips is lost when the power is turned off.

Reverse Address Resolution Protocol (RARP)

The protocol that translates an Ethernet address into an Internet address. This protocol is needed for your unit to discover its Internet address from the network.

ROM

Read Only Memory. Memory chips that cannot be written to after they are manufactured. These chips are used to store permanent system information.

RS232

A type of communication over a serial cable characterized by serial binary data interchange.

Server

A station on a network providing a service, such as making a files or printers available.

SLIP

Serial Line Internet Protocol, a protocol that allows IP protocol to be used over an asynchronous RS-232-C port.

TCP/IP

Transmission Control Protocol/Internet Protocol. The type of communication used by UNIX machines connected to an Ethernet network. TCP provides reliable communication among computers once the data link is established. IP provides the services necessary to manage the movement of data through a computer network, including address resolution, routing, and switching.

Telnet

An application for remote terminal connection service. Using Telnet, a terminal can interact with any host on a network to which it is not directly connected. Telnet is accessed through the terminal's remote login window.

TFTP

Trivial File Transfer Protocol. One of the ways to transfer files between machines connected to an Ethernet network.

Transceiver

A device that connects devices to a Thick Ethernet network. A transceiver contains anti-collision firmware. It is needed on a Thick Ethernet network because of the volume of data on such a network.

Thick Ethernet

A network using thick coaxial cable.

Thin Ethernet

A network using thin coaxial cable.

User Datagram Protocol (UDP)

A simple datagram protocol layered above the Internet protocol.

INDEX

A

Add Printer, 56, 57
ASCII, 63, 64, 66, 69, 95
attributes, 10, 18, 81
Authentication, 7, 8, 10, 19, 20, 30, 43, 87
Auto Mount, 16, 20

B

Binary, 63, 64, 66, 69, 95, 99
BROWSE, 6, 17, 25, 28, 29, 38, 56, 57, 87, 93
Buffer Size, 9, 18, 31, 37

C

cache, 9, 18
Cache Off, 9, 18
Color Mapping, 81
Character Mapping, 32

D

default user, 8
Disable NFS 3.0, 9, 18
Domain Name Server, 42
DOS to UNIX File Conversion, 37

F

File Attribute, 10, 18
File locking, 30, 85, 86
File Permission, 36
FTP Client, 41, 61, 63
FTP Server, 59, 60, 61, 63, 64, 69

G

GID, 8, 12, 19, 29, 35, 36, 43, 87, 71, 78

H

Host Editor, 6, 7, 15-17, 19, 20, 34, 41, 42, 44, 53, 82
Host Name, 12, 34, 41, 42, 54, 64, 71, 82, 83, 90

I

IP address, 42, 54, 64, 78, 82, 98

K

Keyboard Setup, 77
Keymap, 79, 81
Keypad, 71, 73, 74

L

Locking, 10, 18, 30, 37, 85, 86
LPD Server, 45, 48, 49, 50
LPR Hosts, 53, 56
LPR Printer, 53-57

M

Map Network Drive, 12, 20
mapping, 6, 8, 10, 12, 27-29, 32-37, 70, 79, 81, 94
mount, 8-11, 16, 18, 20, 22, 25, 27, 35-38, 40, 44, 45, 85, 86, 91, 94,96
Multiple Session, 70

N

Network Neighborhood, 15, 20, 44, 53
Network Printers, 55-57
NFS client, 1, 5, 10, 15, 16, 21, 23, 27-30, 33, 36, 37, 41, 42, 85, 86, 87, 93
NFS Printer, 30, 32, 37, 38, 55-57
NFS Server, 2, 5-10, 12-15, 19-43, 55, 56, 91-94
NIS Setup, 42, 43
NLM File Locking, 85

O

Options, 5, 9, 17, 29, 37, 46, 66, 75, 79

P

PCNFSD, 7, 19, 30, 36, 37, 43, 55, 57, 87, 88
permission, 7, 8, 10, 19, 25, 34-37, 56, 59, 69, 87, 98
Port Mapper, 37
Print Spooling, 45, 88, 90
Printer Setup, 78, 79, 89
protocol, 1, 63, 85, 87, 95, 98, 100

R

R/W List, 34
Read Only, 34, 86, 99
Read/Write, 34-36
Reconnect At Logon, 20
Remote Printer, 45, 54, 55, 89
RSH, 36, 83, 84, 93

S

SCO System, 56
Security Mapping, 34-36
server Gateway, 13, 14, 93
sharing, 1, 13, 24, 85
Symbolic Link, 21

T

Telnet, 70, 71, 82, 100
Terminal, 70-77, 96, 97, 100
Terminal Emulation, 70
Terminal ID, 73
Time out, 60, 66

U

UID/GID, 12, 36, 43, 87
UNIX Hosts, 3, 84
user, 1-16, 19, 20, 23, 24, 27-29, 32, 34-37, 43-45, 48-51, 59-64, 69, 73, 74, 78-87, 93-97, 100, 101
User Denied Keys (UDK), 73

V

VT420, 1, 41, 70-73, 79-81

W

Windows Explorer, 15, 16, 20, 44